

機能詳細編

LAN側の設定	1
セキュリティの設定	45
LAN側パソコンサーバ公開設定	99
VPNの設定	127
保守・管理	159

LAN側の設定

ここでは、主に本製品のLAN側の設定について解説します。

IPアドレスの設定

本製品のLAN側ポートのIPアドレスを確認・変更する方法を解説します。

ご注意

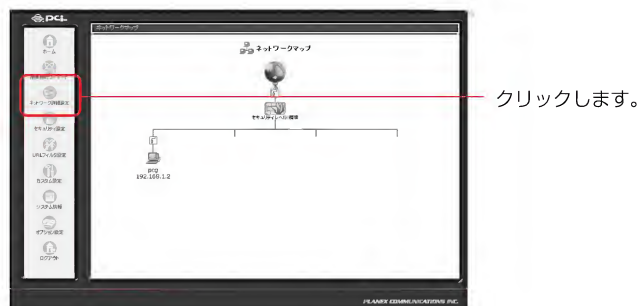
本製品のIPアドレスを変更する場合は、誤ったIPアドレスを設定することのないようご注意ください。誤ったIPアドレスを設定すると、インターネットに接続できなくなるなどのトラブルになることがあります。

LAN側ポートのIPアドレスを確認・変更する

購入時の状態では、本製品のLAN側ポートのIPアドレスは「192.168.1.1」が設定されています。

すでにLANが構築されている環境に本製品を導入した場合などで、本製品のLAN側ポートのIPアドレスを変更する必要があるときは、次の手順で行います。

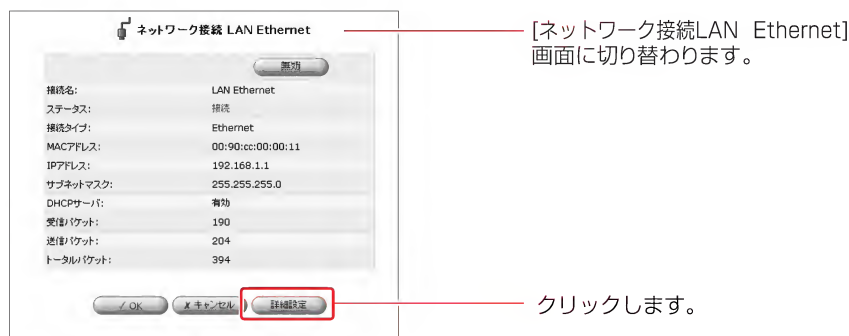
- 1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします。



- 2 [LAN Ethernet] の、修正ボタンをクリックします。



- 3 [詳細設定] ボタンをクリックします。

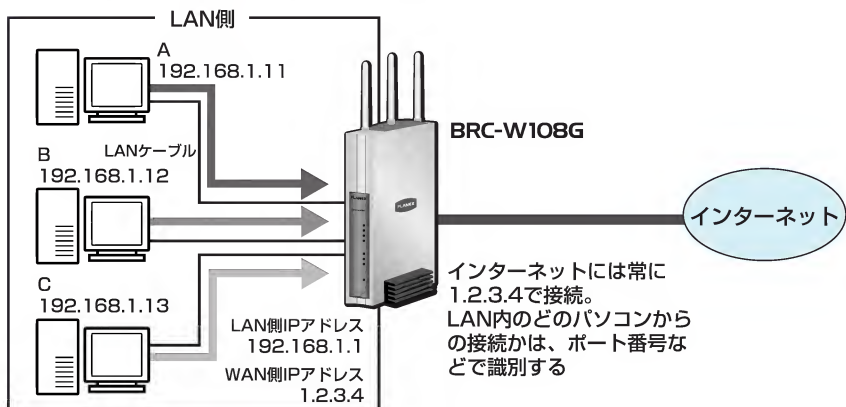


NAPT (IP マスカレード)

本製品では、ルーティングのモードとしてNAPTに対応しています。

複数のプライベートIPアドレスを1つのグローバルIPアドレスに変換する機能で、IP マスカレードとも呼ばれます。LAN側にプライベートIPアドレスを割り当てたパソコンが複数台あり、1つのグローバルIPアドレスでインターネットに接続する運用形態のときは、NAPTを使用します。

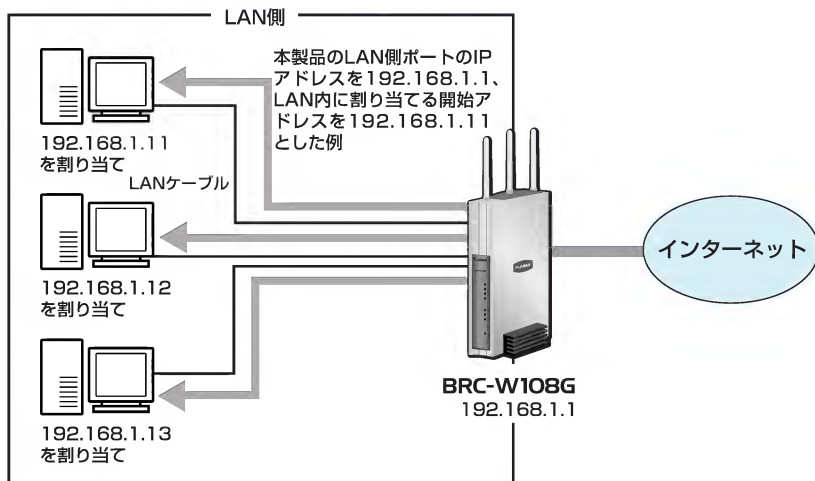
NAPTを使用した場合、LAN内で割り当てられてる複数のプライベートIPアドレスが、インターネットへの接続時に1つのグローバルIPアドレスに変換されます。さらに、ポート番号も変換されます。インターネット側からは、常に1台のパソコンがインターネットに接続しているように見えます。



※NAPT機能を利用するための設定は必要はありません。本製品の運用を開始すると、自動的にNAPT機能は有効になります。

DHCP サーバ設定

DHCP サーバ機能を利用すると、LAN 内のパソコンやネットワーク機器が LAN に接続されるたびに、他のどれとも重複しない IP アドレスを自動で割り当てることができます。



本製品のDHCPサーバ機能は、特定のパソコンに常に固定のIPアドレスを割り当てることもできます。

また固定のIPアドレスの割り当てと、動的なIPアドレスの割り当ての両方を設定することもできます。

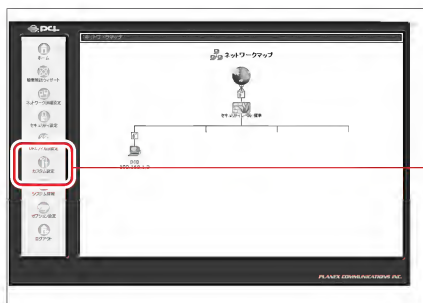
！ ご注意

- ・ 本製品のDHCPサーバ機能はデフォルトで有効になっています。
- ・ DHCPサーバ機能を使用しないときは、LAN側に接続されているパソコンすべてに、手動でIPアドレスを割り当ててください。
- ・ パソコンに手動でIPアドレスを設定した場合、そのパソコンのホスト名やIPアドレスを本製品で管理することはできません。

DHCPサーバの基本設定

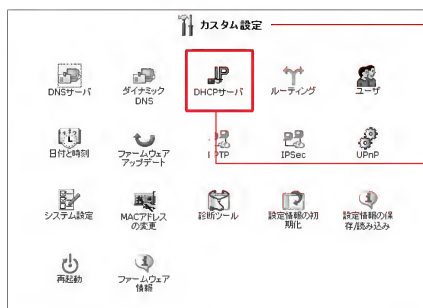
ここでは、DHCPサーバの基本的な設定について説明します

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

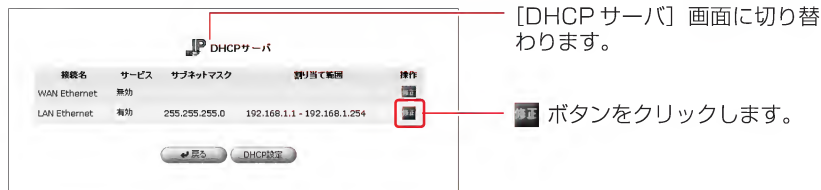
- 2 [DHCPサーバ]アイコンをクリックします。



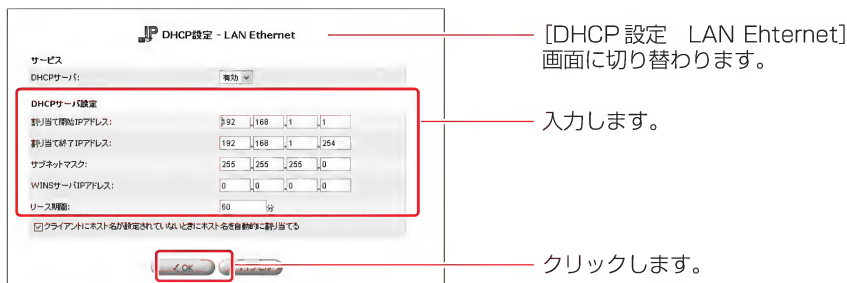
「カスタム設定」画面に切り替わります。

クリックします。

- 3** 現在のDHCPサーバのサブネット、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、修正ボタンをクリックします。



- 4** [DHCP設定 LAN Ethernet]の画面が表示されます。割り当てるIPアドレスの範囲、サブネットマスク、リース期間を設定し、[OK]ボタンをクリックします。



[有効]

DHCPサーバ機能を有効にします。

[割り当て開始アドレス]

割り当てるIPアドレスの、開始アドレスを入力します。

[割り当て終了アドレス]

割り当てるIPアドレスの、終了アドレスを入力します。

[割り当てサブネットマスク]

割り当てるサブネットマスクを入力します。

[WINSサーバ]

WINSサーバを使用してる場合は、サーバアドレスを入力します。

[リース期間 (分)]

割り当てるIPアドレスの有効期限を分単位で入力します。

[クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる]

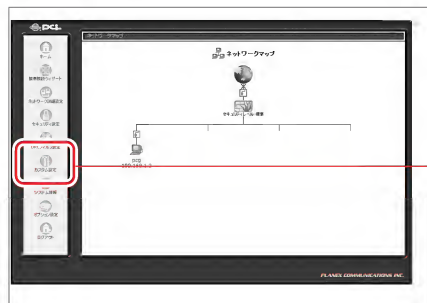
接続されているパソコンまたはネットワーク機器にホスト名が設定されていない場合自動的にホスト名が設定されます。

- 5 [OK]ボタンをクリックし、[DHCPサーバ]画面に戻ります。
- 6 以上で設定は終了です。

DHCPサーバから固定のIPアドレスを割り当てる

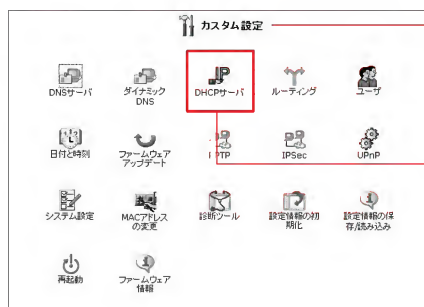
ここでは、特定のパソコンやネットワーク機器にDHCPサーバから常に固定のIPアドレスを割り当てる方法について説明します。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [DHCPサーバ]アイコンをクリックします。



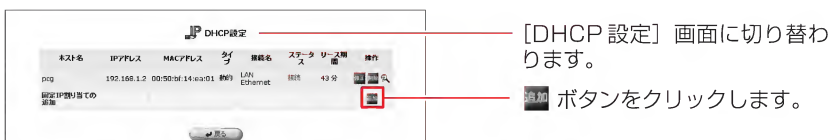
[カスタム設定] 画面に切り替わります。

クリックします。

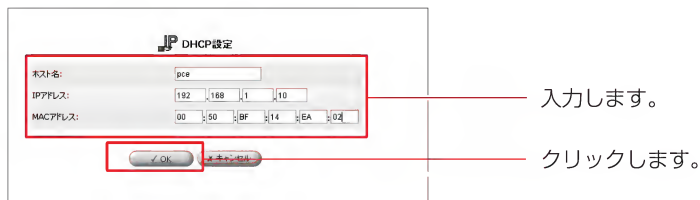
3 [DHCP 設定]ボタンをクリックします。



4 [固定IP割り当ての追加]欄から追加ボタンをクリックします。



5 追加したいパソコンやネットワーク機器のホスト名、IPアドレス、MACアドレスを入力し、[OK]ボタンをクリックします。



[ホスト名]

パソコンまたはネットワーク機器のホスト名を入力します。半角英数字を使用し、1～63文字の範囲で入力してください。

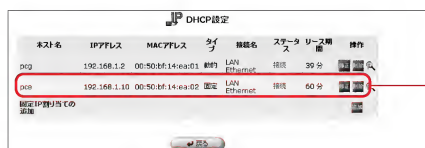
[IPアドレス]

パソコンまたはネットワーク機器に割り当てるIPアドレスを入力します。

[MACアドレス]

IPアドレスを割り当てるパソコンまたはネットワーク機器のMACアドレスを入力します。

6 追加したホストが[DHCP設定]画面に表示されているのを確認します。



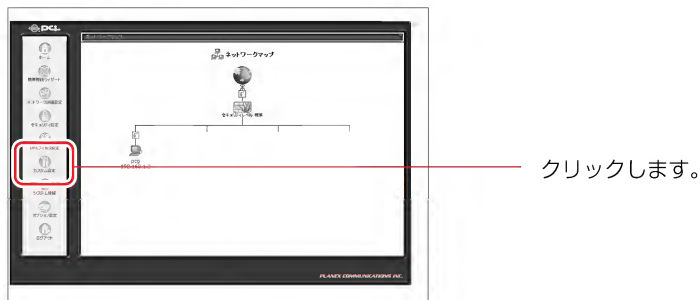
確認します。

7 以上で設定は終了です。

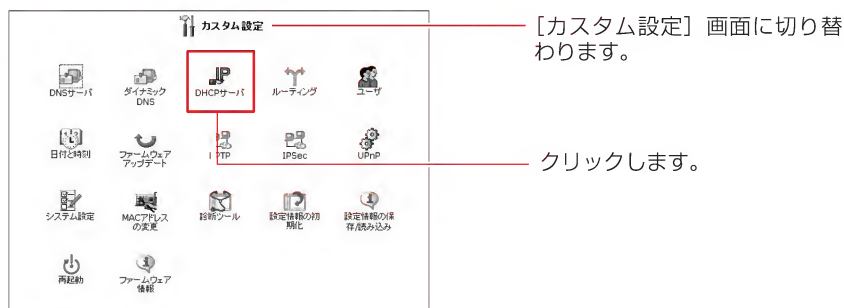
IPアドレスの修正

ここでは、既にDHCPサーバから自動にIPアドレスが割り当てられているパソコンまたはネットワーク機器の設定を変更する方法について説明します。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



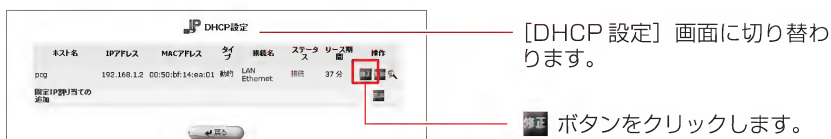
- 2 [DHCPサーバ]アイコンをクリックします。



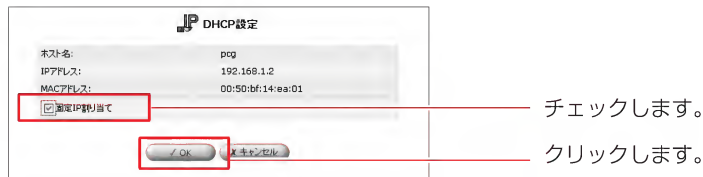
3 [DHCP 設定]ボタンをクリックします。



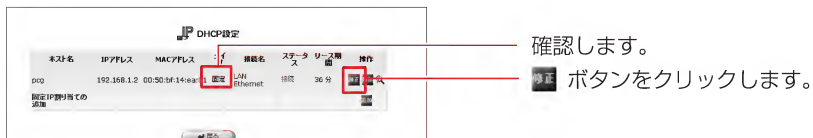
4 設定を変更したいホストの修正ボタンをクリックします。



5 [固定割り当て]にチェックを付け、[OK]ボタンをクリックします。



6 タイプが[固定割り当て]になっているのを確認し、ホストの修正ボタンをクリックします。



- 7** IPアドレスを固定で割り当てたり、ホスト名、MACアドレスの修正を行うことができます。

JP DHCP設定

ホスト名:

IPアドレス:

MACアドレス:

☒ 固定IP割り当て

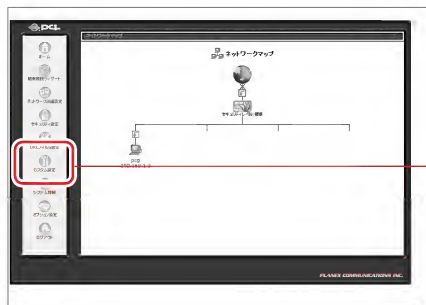
- 8** [OK]ボタンをクリックし、[DHCP 設定]画面に戻ります。

- 9** 以上で設定は終了です。

IPアドレスの削除

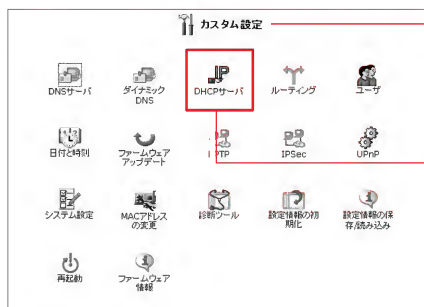
ここでは、登録済みのIPアドレスとホスト名の対応を削除する方法について説明します。

- 1 サイドバーから[カスタム設定]をクリックします。



クリックします。

- 2 [DHCPサーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP 設定]ボタンをクリックします。

[DHCP サーバ] 画面に切り替わります。

接続名	サービス	サブネットマスク	割り当て範囲	操作
WAN Ethernet	無効			
LAN Ethernet	有効	255.255.255.0	192.168.1.1 - 192.168.1.254	

戻る DHCP設定

クリックします。

4 削除したいホストの削除ボタンをクリックします。

[DHCP 設定] 画面に切り替わります。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リリース時間	操作
pc3	192.168.1.2	00:50:57:14:a0:01	静的	LAN Ethernet	有効	43 分	削除

追加

ボタンをクリックします。

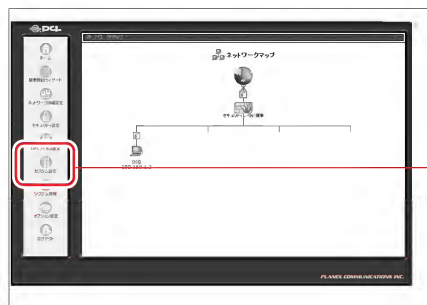
5 [戻る]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

6 以上で設定は終了です。

DHCP サーバ機能の有効/無効を設定する

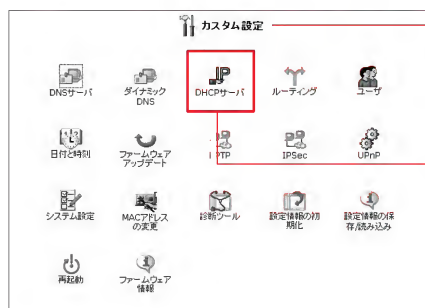
ここでは、DHCPサーバ機能の有効/無効を設定する方法について説明します。

- 1 サイドバーから[カスタム設定]をクリックします。



クリックします。

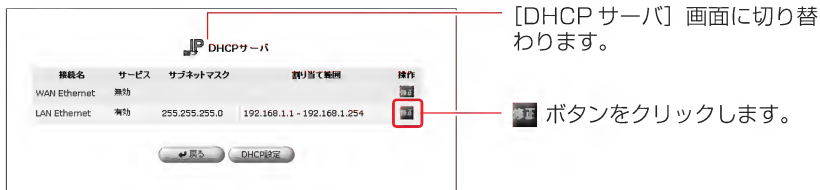
- 2 [DHCPサーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

- 3** 現在のDHCPサーバのサブネット、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、修正ボタンをクリックします。



- 4** [DHCP サーバ] 欄から[有効]または[無効]を選択します。



! ご注意

- ・ DHCP サーバ機能を無効にした場合は、本製品のLAN側に接続されてるパソコンまたはネットワーク機器に、手動でIPアドレスを設定してください。

- 5** [OK]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

※ [OK] ボタンをクリックして [注意]画面に切り替わる場合には、その内容をご確認の上、さらに [OK] ボタンをクリックして [DHCP サーバ] 画面に戻ってください。

- 6** 以上で設定は終了です。

DNS サーバ設定

本製品のDNSサーバは、LAN内のパソコンやネットワーク機器のホスト名とIPアドレスの対応を管理しています。

DNSサーバはDHCPサーバと同じの対応表を参照しています。DHCPサーバの設定時にホスト名を登録しておく、他に特別な設定をせずに、ホスト名および対応するIPアドレスがDNSサーバで管理されます。

ご注意

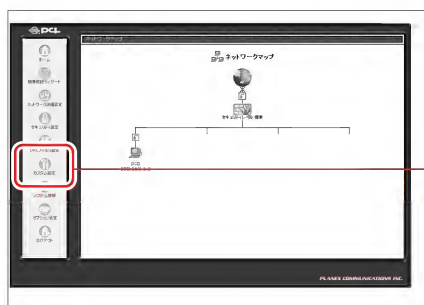
- ・ 本製品のDNSサーバは、LAN内のドメイン名とIPアドレスの対応だけを管理しています。
- ・ インターネット上のドメイン名を指定した通信では、本製品の「プロキシDNS」機能が使用されます。

DHCPサーバによるホスト名とIPアドレスの確認

本製品のDNSサーバはDHCPサーバと同じ対応表を参照しています。
DHCPサーバでホスト名とIPアドレスを登録した場合は、DNSサーバにも反映されます。

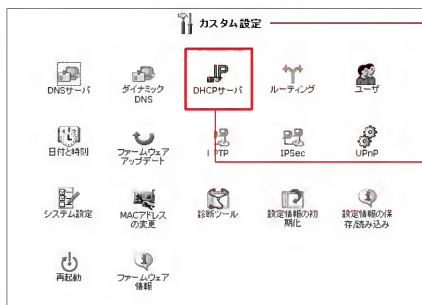
ここでは、DHCPサーバ機能で自動登録されたホスト名とIPアドレスを確認します

- 1 サイドバーから[カスタム設定]をクリックします。



クリックします。

- 2 [DHCPサーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP設定]アイコンをクリックします。



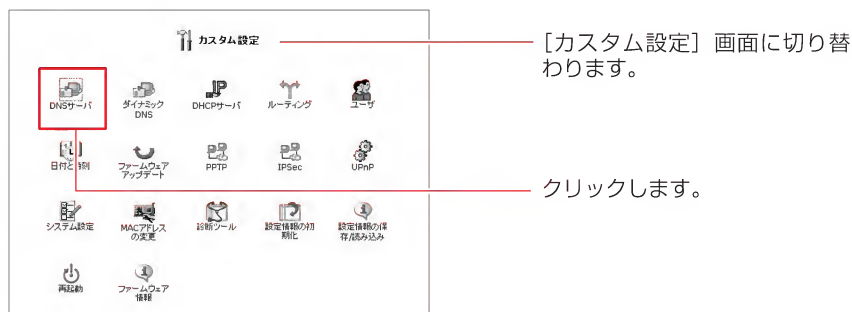
4 DHCPサーバ機能により、本製品に登録されてるホスト名とそのIPアドレスが表示されます。



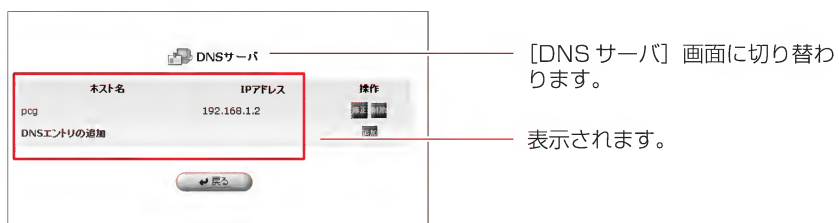
5 [戻る]ボタンをクリックし、[DHCPサーバ]画面に戻ります。

6 [戻る]ボタンをクリックし、[カスタム設定]画面に戻ります。

7 [DNSサーバ]アイコンをクリックします。



8 本製品のDNSサーバに登録されてるホスト名とIPアドレスが表示されます。

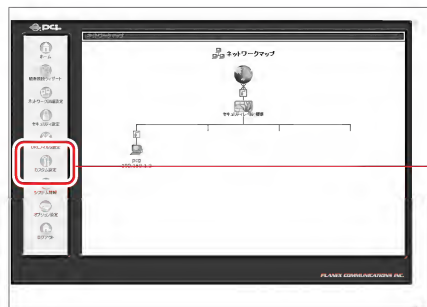


9 以上で確認は終了です。

ホスト名とIPアドレスを手動で登録する

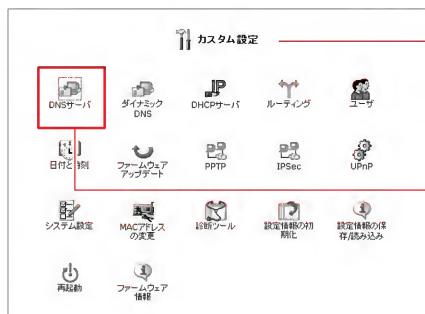
DHCP サーバ機能を使用しない場合は手でホスト名とIPアドレスを登録する必要があります。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

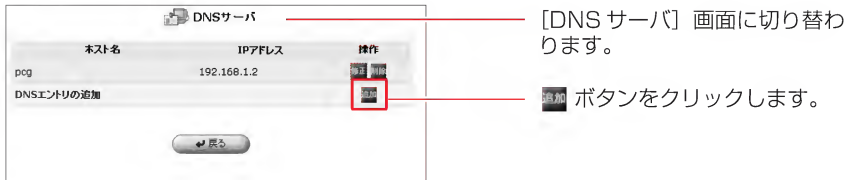
- 2 [DNSサーバ]アイコンをクリックします。



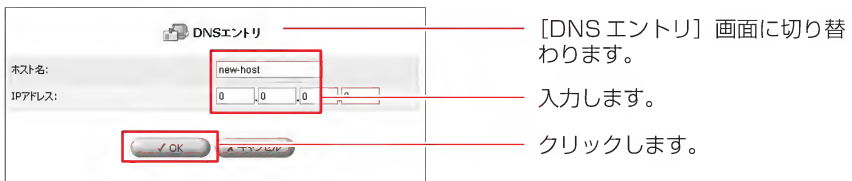
「カスタム設定」画面に切り替わります。

クリックします。

3 [DNSエントリの追加]から追加ボタンをクリックします。



4 DNSサーバに登録するホスト名とIPアドレスを入力し、[OK]ボタンをクリックします。



5 以上で設定は終了です。

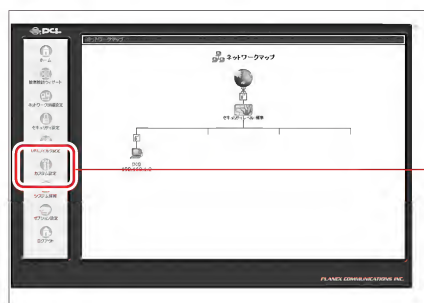
ホスト名とIPアドレスの修正

ホスト名やIPアドレスを変更したときは、DNSサーバに登録した情報も手動で変更する必要があります。

！ ご注意

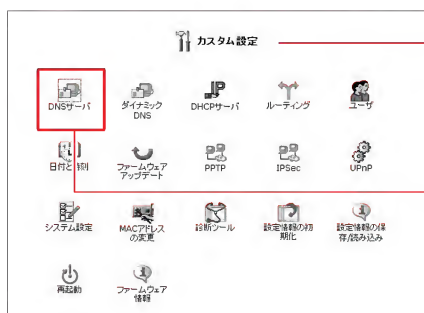
- ・ DHCPサーバ機能を有効にしているときは、パソコンのホスト名は自動的にDNSサーバに反映されます。手動でホスト名を変更する必要はありません。

1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

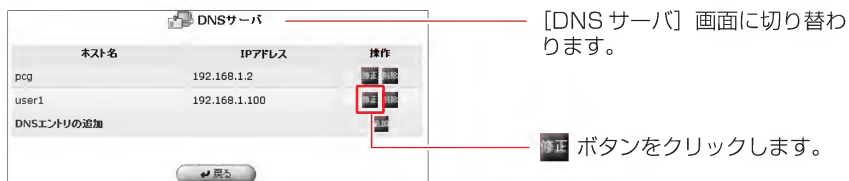
2 [DNSサーバ]アイコンをクリックします。



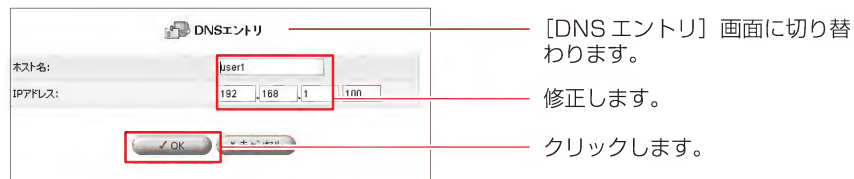
[カスタム設定] 画面に切り替わります。

クリックします。

3 情報を修正したいホスト名の修正ボタンをクリックします



4 ホスト名とIPアドレスを修正し、[OK]ボタンをクリックします。



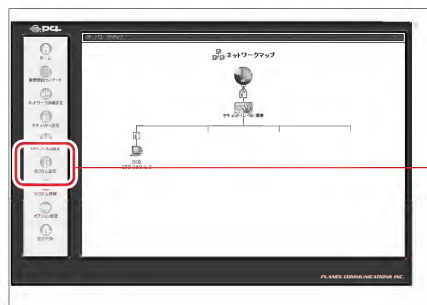
※DHCPサーバによりIPアドレスを割り当てられたホストについては、ホスト名のみ修正が可能です。

5 以上で設定は終了です。

ホスト名とIPアドレスの削除

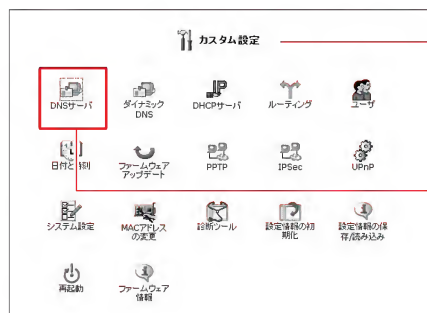
登録されているホスト名とIPアドレスの削除を行います。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [DNSサーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

- 3 情報を削除したいホスト名の削除ボタンをクリックし、[OK]ボタンをクリックします。



[DNSサーバ] 画面に切り替わります。

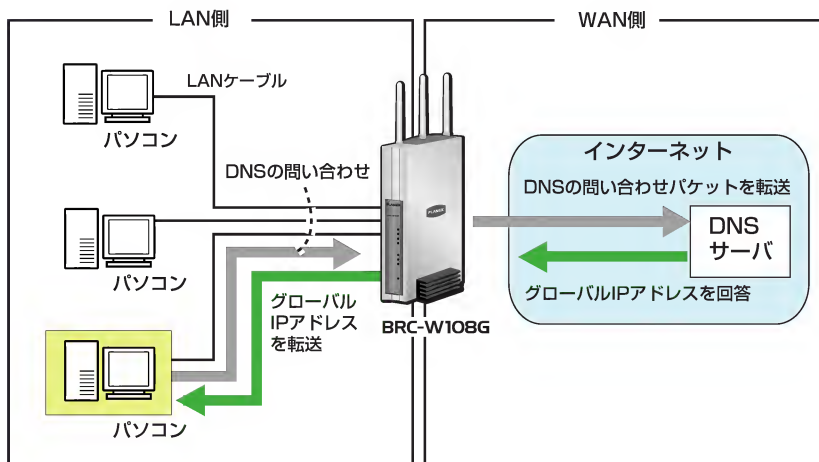
削除 ボタンをクリックします。

クリックします。

- 4 以上で設定は終了です。

プロキシDNS

本製品には「プロキシDNS」機能が搭載されています。プロキシDNSとは、LAN側の各パソコンからインターネット上のドメイン名を指定した接続（DNSの問い合わせ）があった場合に、それをインターネット上のDNSサーバにフォワーディングして、対応するIPアドレスを各パソコンに回答する機能です。LAN側のパソコンからは、インターネット上のDNSサーバに代理で問い合わせていることはわからず、単に、本製品がインターネット上のドメインと各IPアドレスの対応を管理するDNSサーバとして動作しているように見えます。



WAN側で複数セッションを接続している時には、LAN側のパソコンからDNSの問い合わせがあった場合、本製品のプロキシDNS機能は、全てのセッション上のDNSサーバに問い合わせのパケットを送信します。この場合、返答のあったDNSサーバのセッションを使用して通信を行います。2つ以上のセッションのDNSサーバから返答があった場合は、先に返答があった方のセッションを使用します。

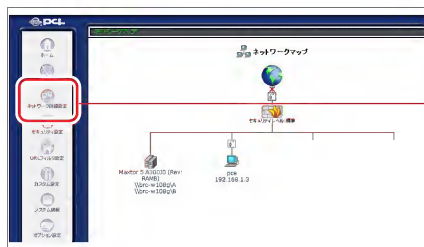
ルーティング設定

本製品は、ダイナミックルーティングのプロトコルとしてRIP、RIP Version2に対応しています。また、スタティックルーティングにも対応しています。

ダイナミックルーティングの設定

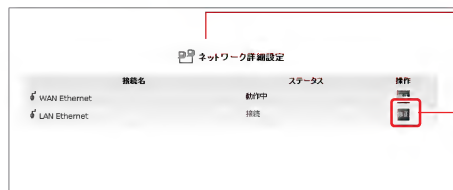
ここでは、ダイナミックルーティングを設定し、動的に経路情報を登録する方法について説明します。本製品のダイナミックルーティングを設定する場合は、ダイナミックルーティングを有効にするインターフェイスを設定し、本製品のダイナミックルーティング機能を有効にします。

- 1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします。



クリックします。

- 2 [接続名]欄からダイナミックルーティングを有効にするインターフェイスの修正ボタンをクリックします。



[DHCPサーバ] 画面に切り替わります。

修正 ボタンをクリックします。

- 3 ここでは例として [LAN Ethernet]を選択します。他のインターフェイスを選択し場合は同様の手順でお進めください。

- 4 [ネットワーク接続 LAN Ethernet]画面が表示されます。[詳細設定] ボタンをクリックします。



- 5 [デバイスメトリック] 欄から [RIP-ルーティングプロトコル] にチェックをつけます。



- 6 RIP の送受信設定を行います。[RIP 受信設定] 欄から本製品が受信する RIP の種類を選択します。[RIP 送信設定] 欄から本製品から送信する RIP の種類を選択します。



RIP受信設定

なし	RIP機能を無効にします。
RIPv1	RIPv1による、ルート情報の受信を行います。
RIPv2	RIPv2による、ルート情報の受信を行います。
RIPv1/2	RIPv1/2による、ルート情報の受信を行います。

RIP送信設定

なし	RIP機能を無効にします。
RIPv1	RIPv1による、ルート情報の送信を行います。
RIPv2・ブロードキャスト	RIPv2による、ルート情報の送信を行います。
RIPv2・マルチキャスト	RIPv2による、ルート情報の送信を行います。

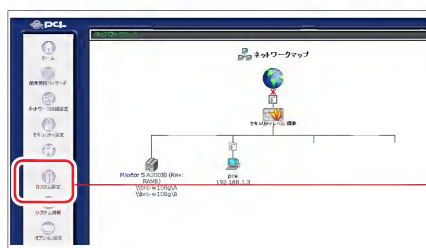
- 7 [OK] ボタンをクリックします。[注意] 画面が表示される場合は、内容を確認したうえで [OK] ボタンをクリックします。



クリックします。

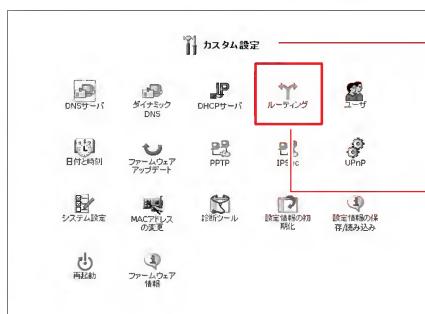
- 8 [ネットワーク接続 LAN Ethernet]画面に戻ります。

- 9 サイドバーから [カスタム設定] アイコンをクリックします。



クリックします。

- 10 [ルーティング] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

- 11** [ルーティングプロトコル] 欄から [RIP-ルーティングプロトコル] にチェックがついてるか確認します。



[ルーティング] 画面に切り替わります。

追加されます。

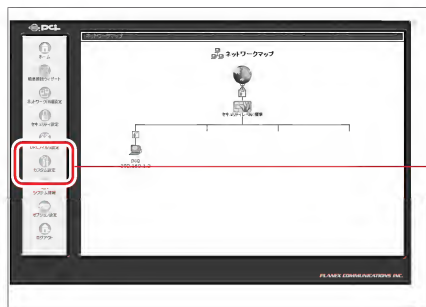
- 12** [OK] ボタンをクリックします。

- 13** 以上で設定は終了です。

スタティックルーティングの経路情報を追加する

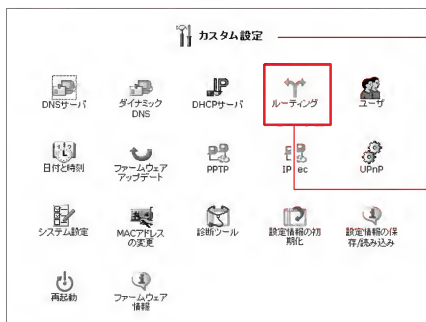
ここでは、経路情報を手動で設定する方法について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

2 [ルーティング]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [ルートの追加]から[追加]ボタンをクリックします。



[ルーティング] 画面に切り替わります。

ボタンをクリックします。

4 経路情報を追加するデバイスを選択し、経路情報を入力します。



[ルーティング設定] 画面に切り替わります。

選択します。

【接続名】

スタティックルーティングを設定する転送先のインタフェースを [LAN Ethernet]、[WAN Ethernet]、[WAN PPPoE] 等から選択します。

【送信先】

パケットの送信先となるネットワークアドレスを入力します。

【ネットマスク】

パケットの送信先のネットマスクを入力します。

【ゲートウェイ】

宛先のネットワークに到達するための、最初のゲートウェイのアドレスを入力します。

【メトリック】

宛先のネットワークに到達するまでのホップカウント(経由するゲートウェイの数)を入力します。

5 [OK]ボタンをクリックします。[ルーティングプロトコル]欄に設定したルーティング情報が追加されます。



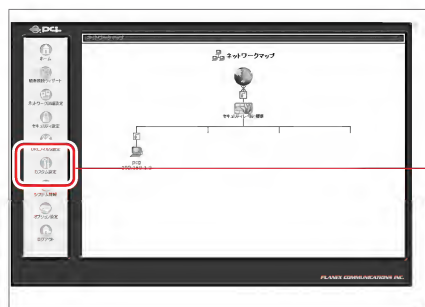
チェックします。

6 以上で設定は終了です。

スタティックルーティングの経路情報を修正する

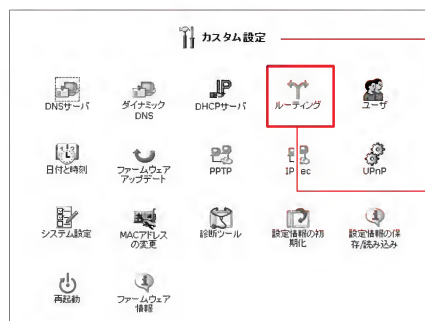
ここでは、既に設定したスタティックルーティングの経路情報を修正する方法について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックする。



クリックします。

2 [ルーティング]アイコンをクリックする。



「カスタム設定」画面に切り替わります。

クリックします。

3 修正したい経路情報の[修正]ボタンをクリックします。

接続名	送信先	ゲートウェイ	ネットマスク	メトリック	ステータス
LAN Ethernet	192.168.10.0	192.168.1.100	255.255.255.0	2	追加された

ルーティングプロトコル

☐ RIP - ルーティングプロトコル

☐ マルチキャスト

OK キャンセル

[ルーティング] 画面に切り替わります。

修正 ボタンをクリックします。

4 経路情報を修正し、[OK]ボタンをクリックします。

接続名: LAN Ethernet

送信先: 192.168.10.0

ネットマスク: 255.255.255.0

ゲートウェイ: 192.168.1.100

メトリック: 2

OK

[ルーティング設定] 画面に切り替わります。

修正します。

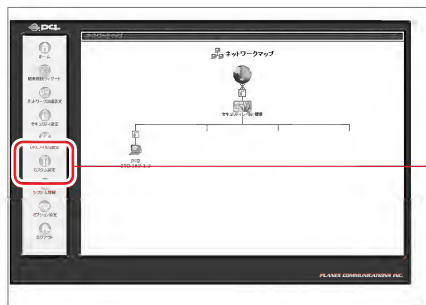
クリックします。

5 以上で設定は終了です。

スタティックルーティングの経路情報を削除する

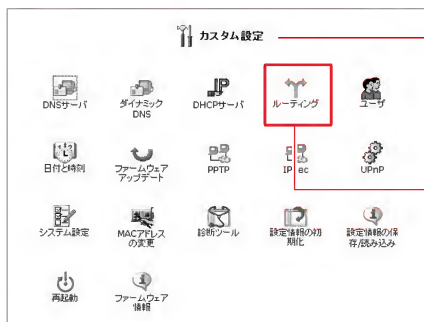
ここでは、登録したスタティックルーティングを削除する方法について説明します。

- 1 サイドバーから[カスタム設定]アイコンをクリックする。



クリックします。

- 2 [ルーティング]アイコンをクリックする。



[カスタム設定] 画面に切り替わります。

クリックします。

3 削除したい経路情報の[削除]ボタンをクリックします。

[ルーティング] 画面に切り替わります。

ボタンをクリックします。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

UPnP 設定

Universal Plug and Play (UPnP : ユニバーサルプラグアンドプレイ) は、ネットワークに接続するだけで、ネットワーク上の機器同士で簡単に通信できるようにする規格です。本製品は、UPnPに対応しており、次の機能を使用できます。

※購入時の設定でUPnPがONになっているため、特別な設定をする必要がありません。

- UPnPに対応しているOS (Windows® XPとWindows® Me) から、本製品を検出できます。
- UPnPに対応しているOS (Windows® XPとWindows® Me) から本製品の状態を確認したり、設定を一部変更できます。
- 本製品に接続されているLAN内のパソコンから、Windows® MessengerやMSN® Messengerなど、UPnPに対応しているアプリケーションを使用することができます。

なお、Windows® 98、Windows® 2000 およびMacintosh® はUPnPに対応していません。したがって、UPnPの機能を使用することはできません。

パソコンのUPnPの設定を確認する

お使いのパソコンが、UPnPが使用できる状態になっているか確認してください。

■ Windows[®] XP の場合

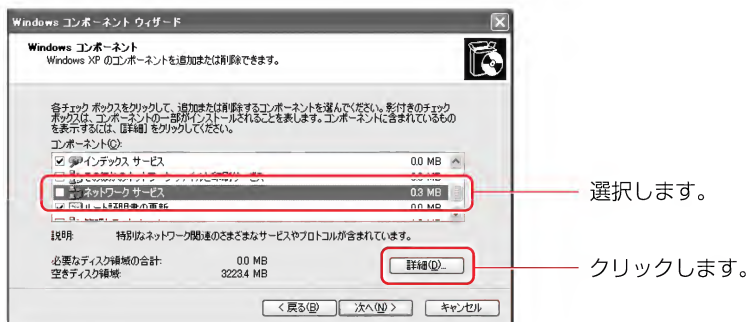
- 1 [スタート] ボタンをクリックし、[コントロールパネル] をクリックします。



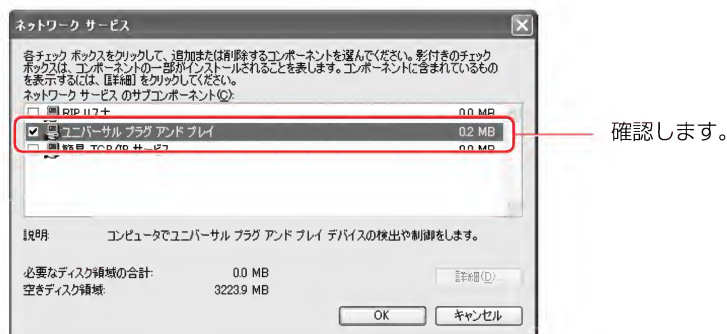
- 2 [プログラムの追加と削除] ボタンをクリックし、画面左側にある [Windows コンポーネントの追加と削除] ボタンをクリックします。



- 3 [コンポーネント] 欄から[ネットワークサービス]を選択し、[詳細] ボタンをクリックします。



- 4 ネットワークサービスの詳細が表示されますので、[ユニバーサルプラグアンドプレイ]の状態を確認します。



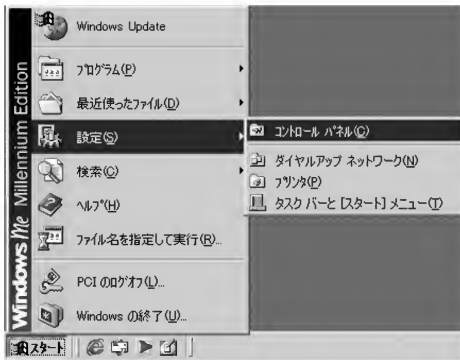
[ユニバーサルプラグアンドプレイ] がチェックされているときは、パソコンが UPnP の機能が有効になっています。ダイアログを閉じてください。

チェックされていないときは、[ユニバーサルプラグアンドプレイ] が無効になっています。チェックを付け、[OK] ボタンをクリックします。画面の指示に従って、インストールを続けてください。

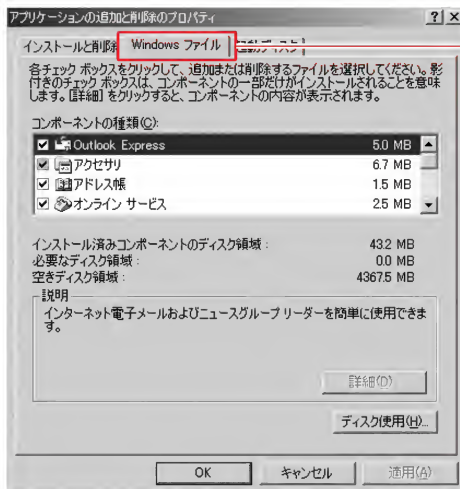
- 5 以上で設定は終了です。

■ Windows® Meの場合

- 1 [スタート] ボタンをクリックし、[設定] → [コントロールパネル] の順にクリックします。

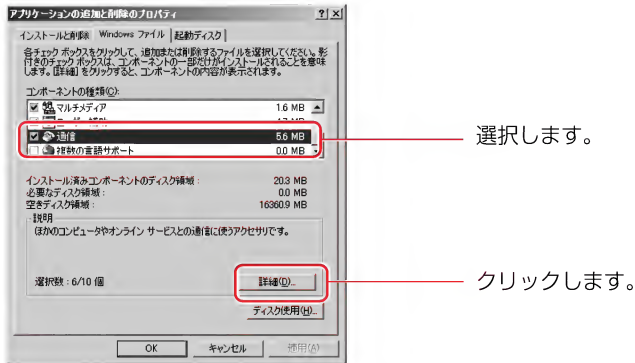


- 2 [アプリケーションの追加と削除] ボタンをクリックします。[アプリケーションの追加と削除] ダイアログが表示されたら、[Windows ファイル] タブをクリックします。

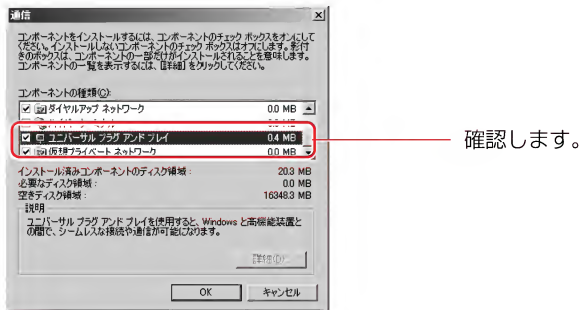


クリックします。

- 3** [コンポーネントの種類] 欄から[通信]を選択し、[詳細] ボタンをクリックします。



- 4** 通信の詳細が表示されますので、[ユニバーサルプラグアンドプレイ]の状態を確認します。

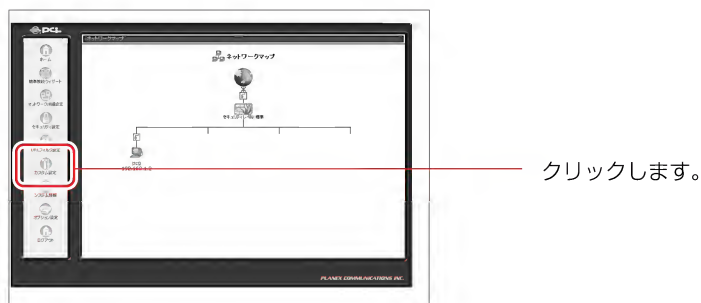


- 5** [ユニバーサルプラグアンドプレイ] がチェックされているときは、パソコンがUPnPの機能が有効になっています。ダイアログを閉じてください。チェックされていないときは、[ユニバーサルプラグアンドプレイ]が無効になっています。チェックを付け、[OK] ボタンをクリックします。画面の指示に従ってインストールを続けてください。
- 6** 以上で設定は終了です。

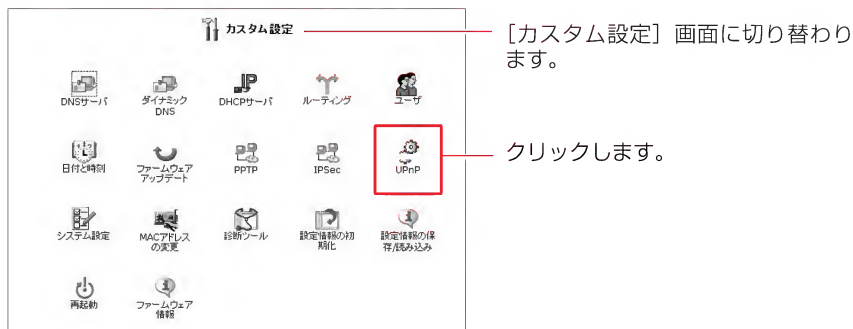
本製品のUPnP機能をOFFにする

本製品でUPnP機能を使用しないときは、次のように操作します。

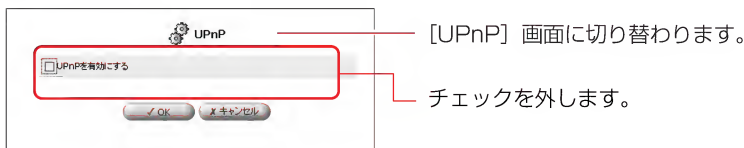
- 1 サイドバーの[カスタム設定]アイコンをクリックします。



- 2 [UPnP]アイコンをクリックします。



- 3 UPnPの機能をOFFにするときは、チェックボックスのチェックを外します。



- 4 [OK] ボタンをクリックします。

- 5 以上で設定は終了です。

セキュリティの設定

セキュリティ機能

インターネットに接続すると、LAN内のパソコンがインターネットからの攻撃を受けたり、不正なアクセスをされたりするという危険があります。そのため、LANを保護する十分なセキュリティ対策を行うことが、快適にインターネットを使う上で重要なポイントとなります。

本製品では、インターネットへの常時接続を行う上でのセキュリティ対策として次の機能を搭載しています。

NAPT (IPマスカレード)	プロバイダから取得したグローバルIPアドレスを、LAN内のプライベートIPアドレスに変換する機能により、インターネット側からLAN内のパソコンを特定できず、アクセスすることができません。このため、外部からの不正アクセスが困難になります。
ステートフル・ パケット・イン スペクション	ファイアウォール方式として、ステートフル・パケット・インスペクション方式を採用しています。通信セッションごとにパケットの整合性を確認し、必要なポートだけを開くようにします。通信が終了すると利用したポートを遮断します。 さらに、インターネット側からのDoS（Denial of Services）攻撃パターンを識別し、不正なアクセスを遮断することが可能です。
ALG (Application Level Gateway)	アプリケーションレベルでパケットの通過・遮断を判断します。
パケットフィル タリング	インターネットから送られてきたパケットを検査して通過させるかどうかを判断する機能です。どのような条件でパケットを通過させるか、遮断するかをプロトコル/ポートごとに任意に設定できます。
バーチャル コンピュータ	LAN内の1台のパソコンをバーチャルコンピュータホストとすると、WAN側からの全ての接続要求がバーチャルコンピュータホストに転送されるようになります。
ID・パスワード によるユーザ認 証	本製品の設定を変更するには、ログインIDとパスワードが必要です。

セキュリティレベル設定

ここでは、本製品の基本的なセキュリティレベルの設定を行います。

セキュリティ対策を考える時は、実際のデータのやり取りの流れに合わせて「LANからインターネットへの通信」と「インターネットからLANへの通信」のそれぞれに対してルールを考える必要があります。

一般的には、LANからインターネットにはアクセスできるようにし、インターネットからLANにはアクセスを拒否するように設定します。

本製品のセキュリティ機能には3段階のレベルがあらかじめ用意されています。さらに、用途に応じて設定をカスタマイズすることができます。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



[セキュリティ設定] 画面に切り替わります。

セキュリティの設定が3段階で用意されています。
購入時の設定では、[セキュリティレベル標準] が選択されています。

2 必要に応じて、レベルを変更します。

セキュリティ レベル	インターネット側からの 接続要求	LAN内のパソコンからの 接続要求
最大	拒否 インターネット側からLANにアクセスできません。ただし、[ローカルサーバ]と[リモートアクセス]画面で設定したサービスは使用できます。	制限あり LAN内のパソコンで、WEBサービス、e-mailなどのよく使うインターネットのサービスのみ使用できます。※
標準	拒否 インターネット側からLANにアクセスできません。ただし、[ローカルサーバ]と[リモートアクセス]画面で設定したサービスは使用できます。	制限なし LAN内のパソコンで、すべてのインターネットのサービスが使用できます。
最小	制限なし インターネットからLANへのアクセスをすべて許可します。	制限なし LAN内のパソコンで、すべてのインターネットのサービスが使用できます。

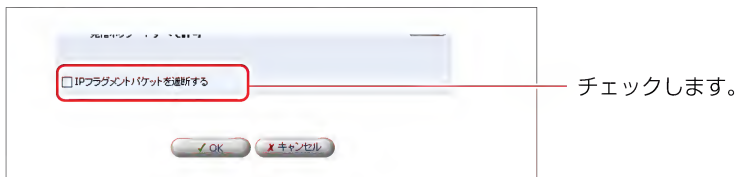
※[セキュリティレベル最大]を選択しているとき、LAN側のパソコンから使用できるインターネットのサービスは次のとおりです。

Telnet、FTP、HTTP、HTTPS、DNS、IMAP、POP3、SMTP

ご注意

[セキュリティレベル最小]を選択すると、セキュリティ機能が一切適用されなくなりますので、必要な場合にのみ設定してください。

3 [IPフラグメントパケットを遮断する]をチェックします。



フラグメント化されたデータパケットを利用した攻撃を防ぐことができます。

※IPSecを利用する仮想プライベートネットワークやUDPをベースにしたサービスによっては、IPフラグメントを利用するものがあります。このようなサービスを利用するときは、チェックを外してください。

4 [OK] ボタンをチェックします。

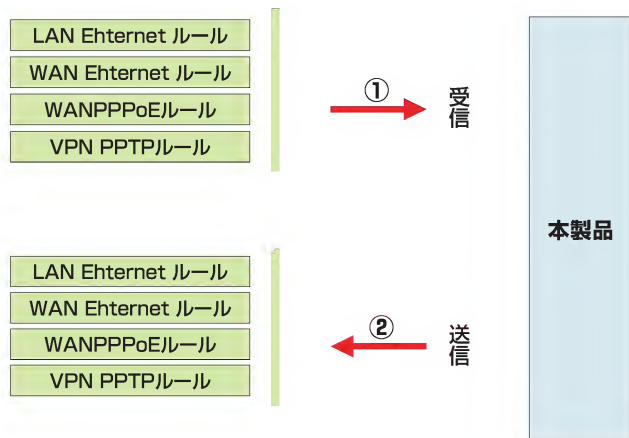
選択したセキュリティレベルに変更されます。

パケットフィルタリング設定

本製品のパケットフィルタの機能は、本製品が受信したパケット、送信するパケットに対してあらかじめ設定してあるフィルタルールを適用します。

フィルタルールには、[LAN Ethernet ルール]、[WAN Ethernet ルール]、[WAN PPPoE ルール]、[WAN PPPoE ルール]等があります。

ルール適用順

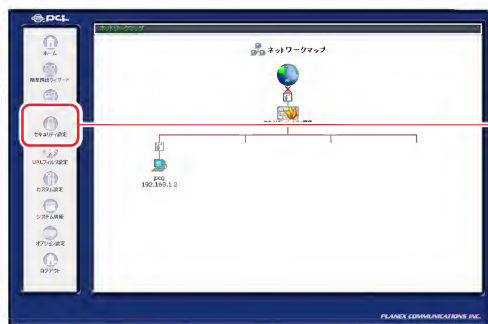


パケットフィルタの設定

ここでは、本製品にパケットフィルタを設定する方法について説明します。

■パケットフィルタの新規設定

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

- 2 [パケットフィルタ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

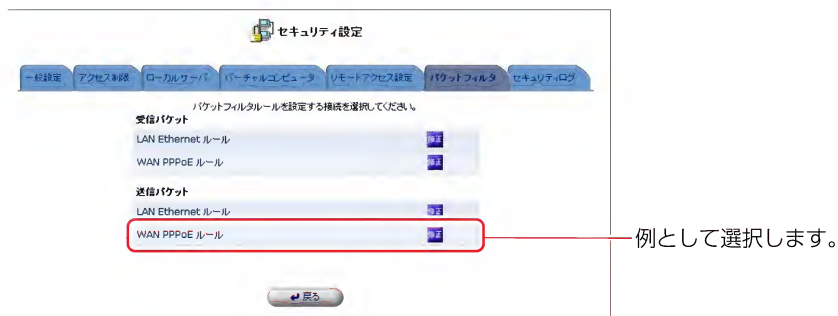
クリックします。

3 [セキュリティ設定]画面が表示されます。



4 [受信パケット]欄、または[送信パケット]欄からルールを作成するインタフェースをクリックします。

※ここでは、例として[WAN PPPoE ルール]を選択します。他のインタフェースを選択した場合は同様の手順で設定してください。



本製品で設定できるルールの一覧

[LAN Ethernet ルール]

LANのポートに対して適用されるルールになります。

[WAN Ethernet ルール]

WANのポートに対して適用されるルールになります。

[WAN PPPoE ルール]

WAN PPPoEのポートに対して適用されるルールになります。

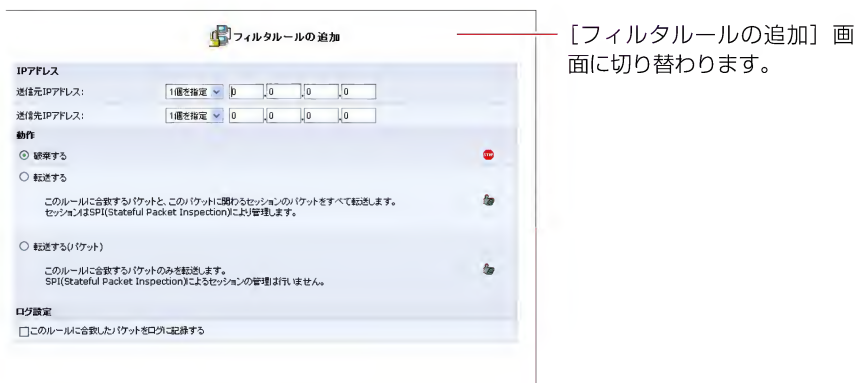
[VPN PPTPルール]

VPN PPTPの接続に対して適用されるルールになります。

- 5** [設定 WAN PPPoE ルール]画面が表示されます。
[新規作成]欄から追加ボタンをクリックします。



- 6** [フィルタルールの追加]画面が表示されます。




7 [IPアドレス]欄から送信元IPアドレス、送信先IPアドレスを入力します。

[すべて]を選択した場合は、全てのIPアドレスが対象になります。



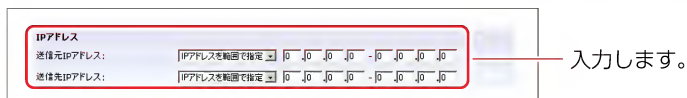
The screenshot shows the 'IPアドレス' (IP Address) section. It has two rows: '送信元IPアドレス:' (Source IP Address) and '送信先IPアドレス:' (Destination IP Address). Both rows have a dropdown menu set to 'すべて' (All). A red box highlights these two rows, and a red arrow points from the text '選択します。' (Select) to the dropdown menus.

[1個を指定]を選択した場合は、指定したIPアドレスが対象になります。



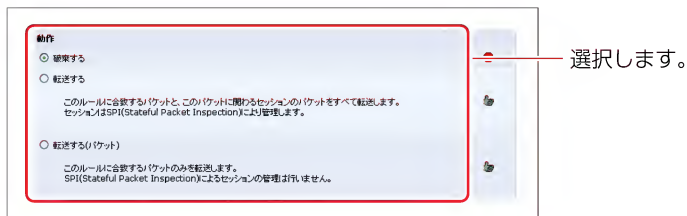
The screenshot shows the 'IPアドレス' (IP Address) section. It has two rows: '送信元IPアドレス:' (Source IP Address) and '送信先IPアドレス:' (Destination IP Address). Both rows have a dropdown menu set to '1個を指定' (Specify 1). To the right of each dropdown are four input fields for IP octets. A red box highlights these rows, and a red arrow points from the text '入力します。' (Enter) to the input fields.

[範囲指定]を選択した場合は、指定したIPアドレスの範囲が対象になります。



The screenshot shows the 'IPアドレス' (IP Address) section. It has two rows: '送信元IPアドレス:' (Source IP Address) and '送信先IPアドレス:' (Destination IP Address). Both rows have a dropdown menu set to 'IPアドレスを範囲で指定' (Specify IP address range). To the right of each dropdown are two input fields for IP ranges. A red box highlights these rows, and a red arrow points from the text '入力します。' (Enter) to the input fields.

8 [動作]欄からフィルタの動作を選択します。



The screenshot shows the '動作' (Action) section. It has three radio button options: '破棄する' (Discard), '転送する' (Forward), and '転送する(パケット)' (Forward (packet)). The '破棄する' option is selected. Below each option is a description. A red box highlights the '破棄する' option, and a red arrow points from the text '選択します。' (Select) to the radio button.

【破棄する】

パケットを破棄します。

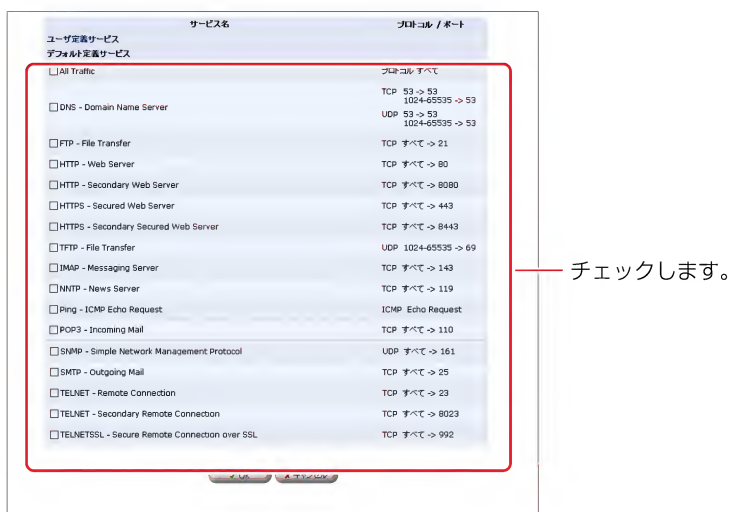
【転送する(セッション)】

このルールに合致するパケットと、このパケットに関わるセッションのパケットを通します。

【転送する(パケット)】

このルールに合致するパケットのみを通します。

- 9** [サービス名]欄に本製品に既に登録されているサービスやアプリケーションが表示されます。フィルタルールの対象となるサービスにチェックをつけます。



- 10** [OK]ボタンをクリックします。



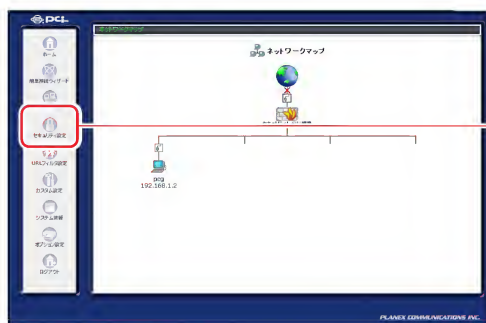
※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

- 11** 複数のフィルタルールを作成する場合は、3～10の手順を繰り返します。

- 12** 以上で設定は終了です。

■パケットフィルタの修正

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

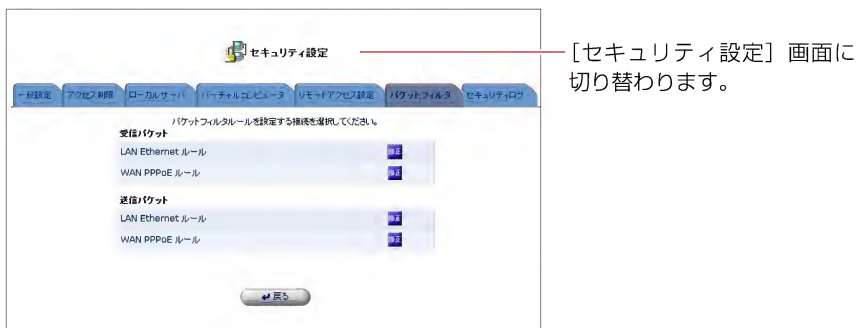
- 2 [パケットフィルタ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

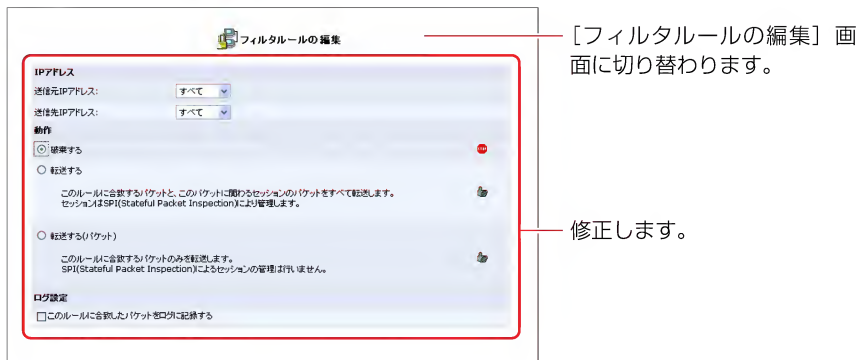
3 設定を変更したいインターフェースの修正ボタンをクリックします。



4 [設定 WAN PPPoE ルール]の画面が表示されますので、[操作]欄から修正ボタンをクリックします。



- 5** [フィルタールの編集]画面が表示されますので、必要な項目の修正を行い[OK]ボタンをクリックします。

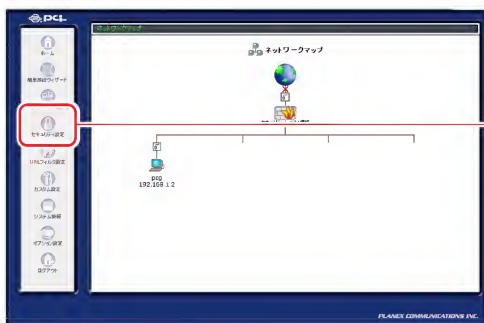


※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

- 6** 以上で修正は終了です。

■パケットフィルタの削除

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

- 2 [パケットフィルタ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

3 設定を削除したいインタフェースの修正ボタンをクリックします。



[セキュリティ設定] 画面に切り替わります。

4 [設定 WAN PPPoE ルール]の画面が表示されます。[操作]欄から削除ボタンをクリックします。



[設定 WAN PPPoE ルール] 画面に切り替わります。

ボタンをクリックします。

5 以上で削除は終了です。

新規にサービスを作成する場合

ここでは、本製品にあらかじめ登録されていないサービスを設定する方法について説明します。

- 1 [フィルタルールの追加]画面から、[ユーザ定義サービス]をクリックします。

[フィルタルールの追加] 画面に切り替わります。

クリックします。

- 2 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から追加ボタンをクリックします。

[ユーザ定義サービス] 画面に切り替わります。

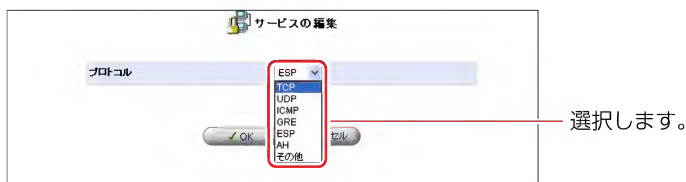
ボタンをクリックします。

- 3 [サービスの編集]画面が表示されます。[新規作成]欄から追加ボタンをクリックします。

[サービスの編集] 画面に切り替わります。

ボタンをクリックします。

4 [プロトコル]欄から使用するプロトコルを選択します。



[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。

[発信元ポート/送信先ポート]

サービスやアプリケーションの発信元ポート/送信先ポート番号を入力します。

- すべて → 全てのポートを指定します。
- 1個を指定 → 1つのポート番号を指定します。
- 範囲指定 → ポート番号の範囲を指定します。

[ICMPメッセージ]

対象にするICMPメッセージを選択します。

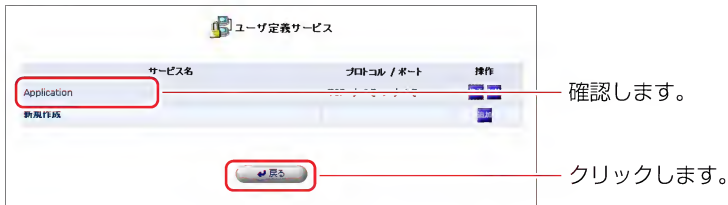
5 [OK]ボタンをクリックします。

6 追加ボタンをクリックすることで、複数のポートを指定することもできます。



7 全ての設定が終了しましたら [サービス名] に任意の名前を入力し、[OK]ボタンをクリックします。

- 8 [ユーザ定義サービス] の画面に戻ります。[サービス名] 欄に作成したユーザ定義サービスが表示されるのを確認します。
[戻る] ボタンをクリックします。



- 9 新規に作成したサービスが[ユーザ定義サービス]欄に表示されます。



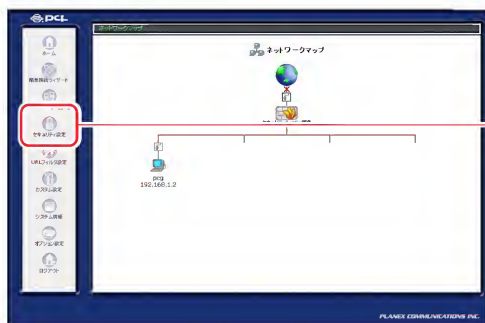
- 10 以上で設定は終了です。

フィルタールの例

ここでは、パケットフィルタの例としてNetBIOS 関連で使われてるポート 137～139のLANからWANへの通信を遮断する方法について説明します。

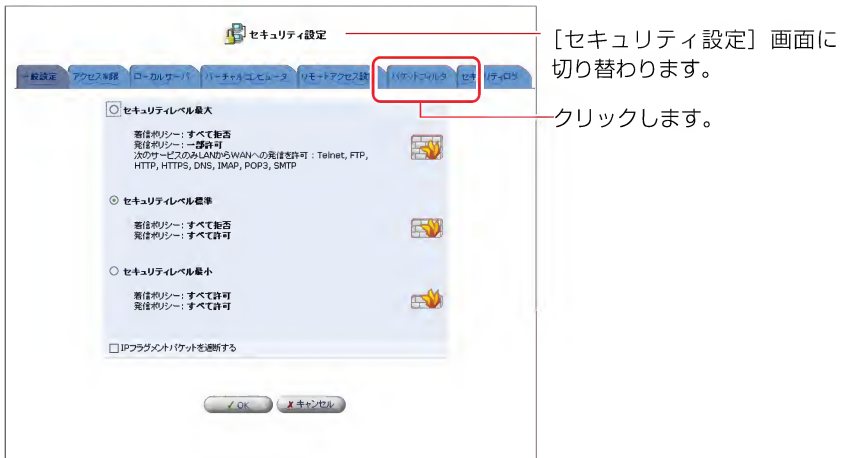
方向	動作	プロトコル	送信元 IPアドレス	送信先 IPアドレス	送信元 ポート	送信先 ポート
LAN Ehternet →受信	破棄	TCP/ UDP	すべて	すべて	すべて	137～139
送信→ WAN Ehternet	破棄	TCP/ UDP	すべて	すべて	すべて	137～139

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

2 [パケットフィルタ]タブをクリックします。



3 LAN側からWAN側へのNetBIOSの packets を遮断するルールを作成します。 [受信パケット]欄から[LAN Ethernet ルール]の修正ボタンをクリックします。



4 [新規作成]欄から追加ボタンをクリックします。



「設定 LAN Ethernet ルール」画面に切り替わります。

追加 ボタンをクリックします。

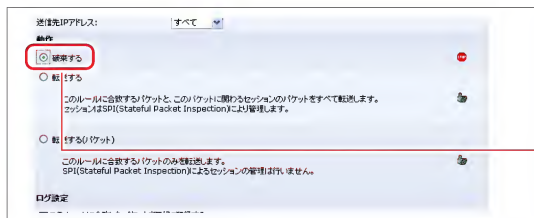
5 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。



「フィルタルールの追加」画面に切り替わります。

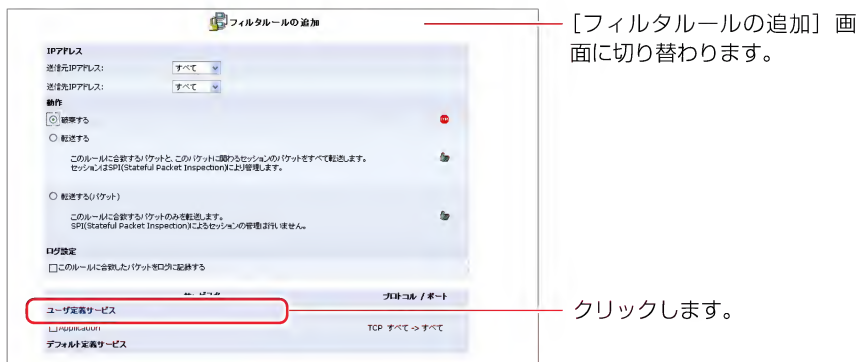
選択します。

6 [動作]欄から[破棄する]にチェックを付けます。

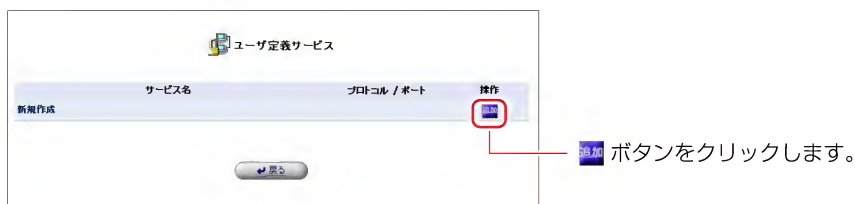


チェックします。

7 [ユーザ定義サービス]をクリックします。



8 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から追加ボタンをクリックします。



9 [サービスの編集]の画面が表示されます。[新規作成]欄から追加ボタンをクリックします。



- 10** プロトコルから[TCP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に137～139を入力します。



- 11** [OK]ボタンをクリックします。

- 12** 同様にUDPポートも遮断しますので、追加ボタンをクリックします。

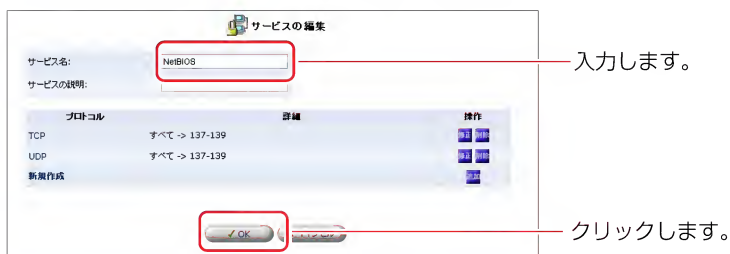


- 13** プロトコルから[UDP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に137～139を入力します。



- 14** [OK]ボタンをクリックします。

- 15** [サービスの編集] 画面が表示されますので、サービス名に登録する名前を入力し、[OK] ボタンをクリックします。



- 16** [ユーザ定義サービス] 画面に戻ります。[サービス名] 欄に作成したユーザ定義サービスが表示されるのを確認します。[戻る] ボタンをクリックします。



- 17** [ユーザ定義サービス]欄に作成したサービスが表示されますので、チェックを付け[OK]ボタンをクリックします。



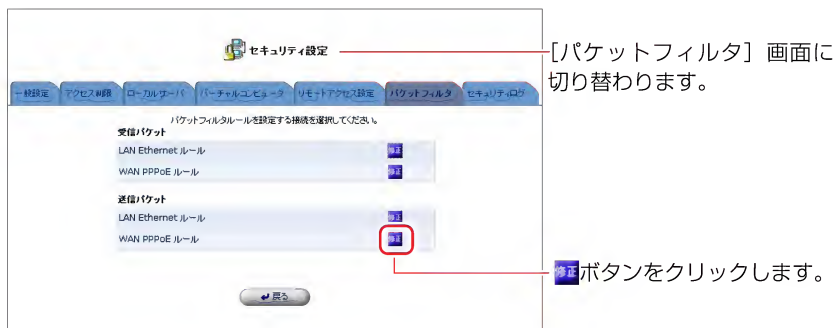
※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

18 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。



19 [OK]ボタンをクリックします。

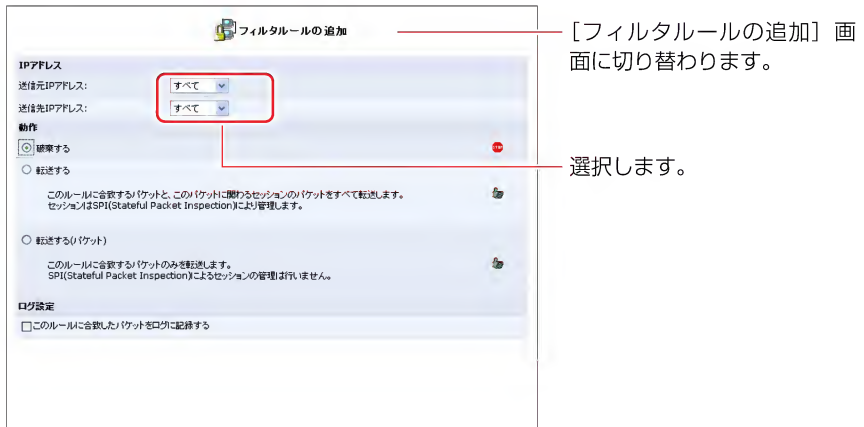
20 次に送信パケットの設定を行います。
[送信パケット]欄から[WAN PPPoEルール]の修正ボタンをクリックします。



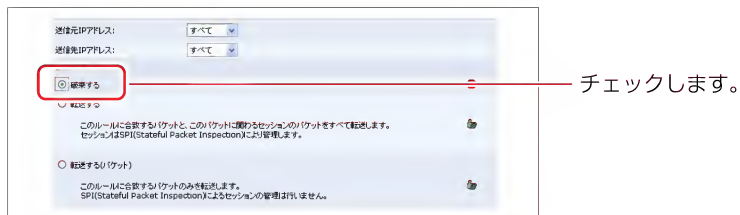
21 [新規作成]欄から追加ボタンをクリックします。



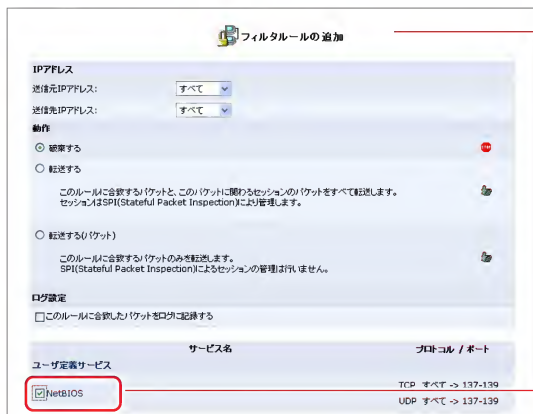
22 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。



23 [動作]欄から[破棄する]にチェックを付けます。



- 22** [ユーザ定義サービス]欄に先ほど作成したサービスが表示されますので、チェックを付け、[OK]ボタンをクリックします。



[フィルタールのルール追加] 画面に切り替わります。

チェックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

- 23** [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。



[設定 WAN PPPoE ルール] 画面に切り替わります。

クリックします。

- 24** 以上で設定は終了です。

リモートアクセス設定

リモートアクセス機能を使うことで、インターネット側から本製品にアクセスし、各種設定を行うことができます。

デフォルト設定では、LANを保護するためにリモートアクセスを許可していません。

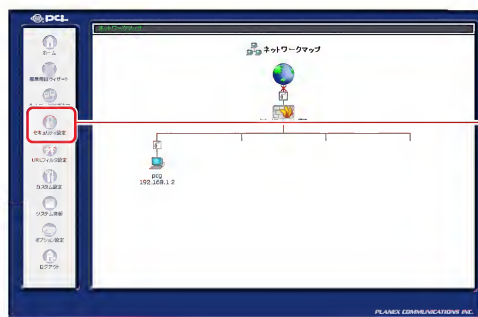
ご注意

不正アクセスにより本製品の設定を変更されないよう、通常はリモートアクセスを無効に設定しておき、必要な場合のみ許可するようにしてください。

本製品に設定されたリモートアクセス機能は、ローカルサーバ、バーチャルコンピュータより優先されます。

リモートアクセスの設定

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

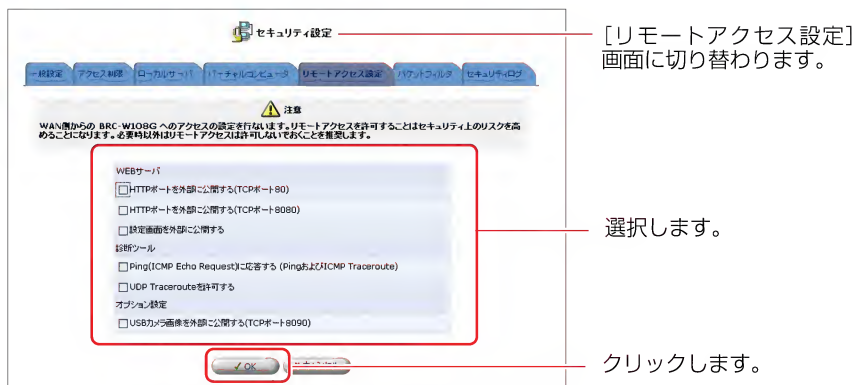
- 2 [リモートアクセス設定]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

3 WAN側からのアクセスに関する設定を行います。



WEB 設定画面	HTTPポートを外部に公開する	本製品のHTTPポートを外部に公開する場合に選択します。
	HTTPポートを外部に公開する(TCPポート8080)	本製品のHTTPポートをTCP8080ポートで外部に公開する場合に選択します。
	設定画面を外部に公開する	本製品の設定画面を外部に公開する場合に選択します。
診断ツール	Pingに応答する	Pingコマンドに返答する場合は選択します。
	UDPを許可	tracertコマンドなどで、UDP上のルート確認をする場合は選択します。
オプション設定		USBカメラから画面を外部に公開する場合に選択します。

ご注意

- Windows® からTracerouteコマンドを使用して、ルートの追跡を行う場合は「Pingに回答する」をチェックしてください。
- 設定画面をWAN側から見るには、以下のURLを指定してアクセスします。
設定画面用アドレス：http://(WAN側アドレス)/setting/

4 [OK] ボタンをクリックします。

5 以上で設定は終了です。

URL フィルタ設定

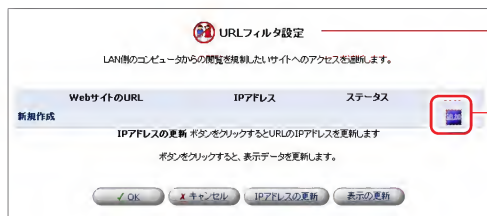
URL フィルタ機能を使うことで、LAN 側のパソコンから特定のWEBサイトを閲覧できないように設定できます。

例えば、公序良俗に反するようなWEBサイトをあらかじめ本製品に設定しておくことで、LAN 側のパソコンからそのサイトの閲覧を禁止することができます。

URL フィルタの設定

■ URL フィルタの新規作成

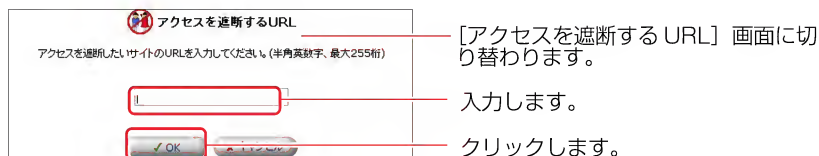
- 1 サイドバーから [セキュリティ設定] アイコンをクリックします。
- 2 [サイトフィルタ] タブをクリックします。
- 3 [新規作成] 欄から追加ボタンをクリックします。



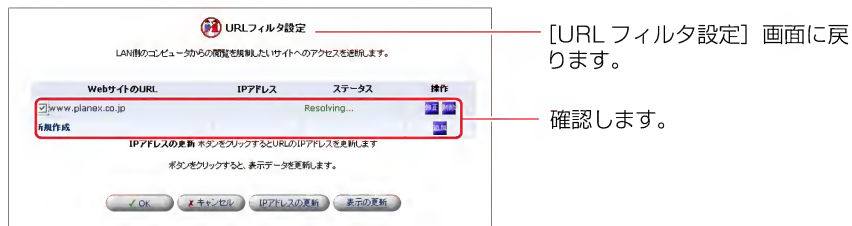
[URL フィルタ設定] 画面に切り替わります。

追加 ボタンをクリックします。

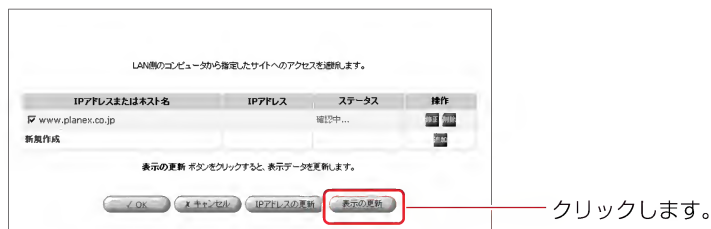
- 4 閲覧を禁止したいWEBサイトのURLまたはIPアドレスを入力し、[OK] ボタンをクリックします。



- 5 [WEBサイトのURL] の一覧に設定したWEBサイトが追加されます。



- 6 URLが追加されると、追加されたURLがインターネット上に存在するか自動的にチェックします。この間、[ステータス] 欄には[確認中]と表示されます。[表示の更新]ボタンをクリックして、入力されたURLが適切なものか確認します。



7 [OK] ボタンをクリックすると、設定が有効になります。

8 以上で設定は終了です。

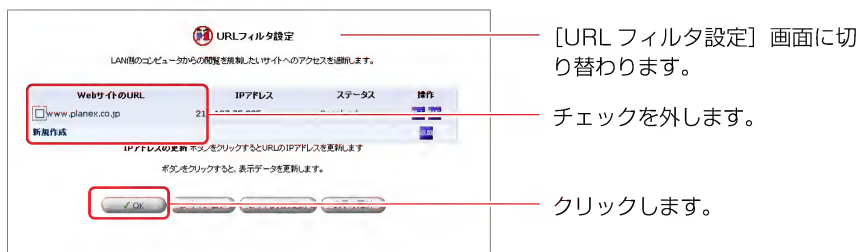
MEMO

ステータスに [Error] が表示される場合

→WEB ブラウザを起動し設定した URL を入力し、WEB ブラウザに表示されるか確認してください。正しく表示されたときは、本製品に設定した URL が間違ってる可能性があります。

■ URL フィルタの有効/無効の切替

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。
- 2 [サイトフィルタ]タブをクリックします。
- 3 [WEBサイトのURL]欄からURLフィルタを無効にしたいWEBサイトのチェックを外し、[OK] ボタンをクリックします。



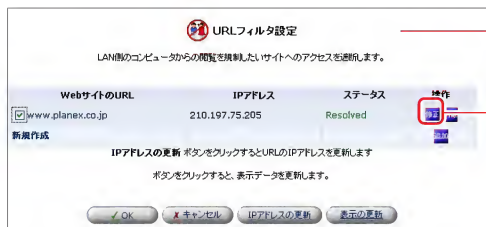
- 4 [サイトフィルタ]を表示します。[ステータス]表示が無効に替わります。再度、URL フィルタを有効にする場合はチェックを付けます。



- 5 以上で設定は終了です。

■ URL フィルタの修正

- 1 サイドバーから [セキュリティ設定] アイコンをクリックします。
- 2 [サイトフィルタ] タブをクリックします。
- 3 設定を変更したいWEBサイトのURLの修正ボタンをクリックします。



[URL フィルタ設定] 画面に切り替わります。

修正 ボタンをクリックします。

- 4 [アクセスを遮断するURL] の画面が表示されましたら、新しいURLまたはIPアドレスを入力し、[OK] ボタンをクリックします。



[アクセスを遮断するURL] 画面に切り替わります。

確認します。

5 [WEBサイトのURL] の一覧に変更したWEBサイトが表示されます。



[URL フィルタ設定] 画面に切り替わります。

確認します。

6 以上で設定は終了です。

■ URLフィルタの削除

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。
- 2 [サイトフィルタ]タブをクリックします。
- 3 設定を削除したいWEBサイトのURLの削除ボタンをクリックします。



削除 ボタンをクリックします。

- 4 [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

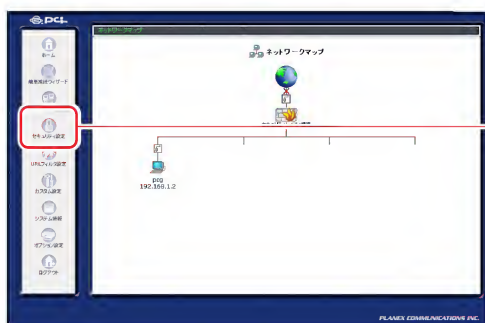
ログの管理

ここでは、LAN側のパソコンからインターネットへの接続やインターネット側からLANへの接続、設定ページへのアクセスなどのログ情報を設定します。

セキュリティログの確認

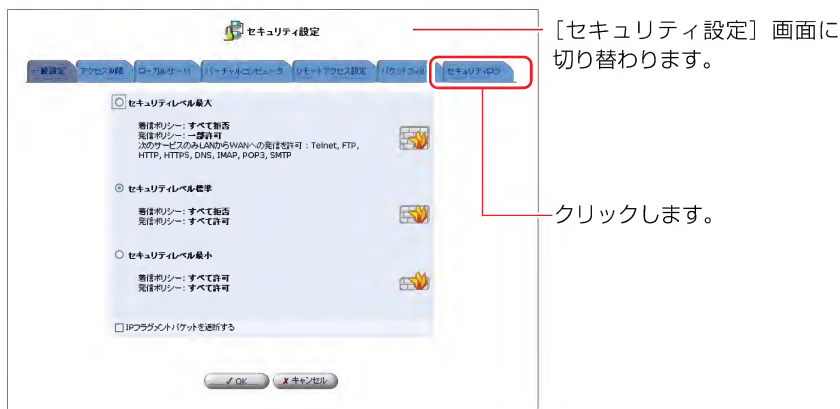
■ログを見る

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。

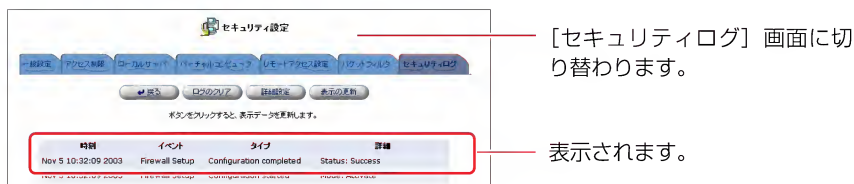


クリックします。

2 [セキュリティログ] タブをクリックします。



3 [セキュリティログ] 画面が表示されます。現在のセキュリティに関するログが確認できます。



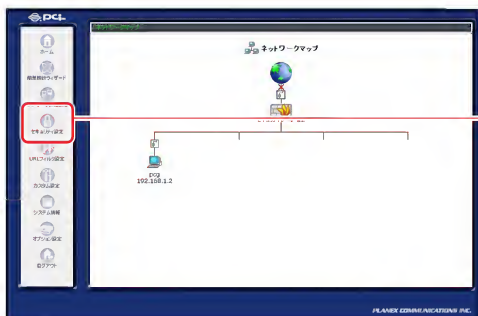
■ログの見方 (例)

イベント	種類	説明
Inbound/ Outbound Traffic	Connection accepted	接続要求がファイアウォールのセキュリティポリシーに適合していた場合に表示されます。
	Accepted - Host probed	ファイアウォールのセキュリティポリシーに適合したTCP接続要求があったが、インターネット側のホストが信頼できるかどうか分からない場合に表示されます。この場合、インターネット側のホストに認証が試みられます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Host trusted	認証を試みていたホストから応答があった場合に表示されます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Internal traffic	すべてのパケットがLAN側のホスト同士の間で自由に行き来できる場合に表示されます。
	Connection Refused- Policy violation	接続要求がファイアウォールのセキュリティポリシーに違反している場合に表示されます。
	Blocked - IP Fragment	ファイアウォールですべてのIPフラグメントをブロックする設定を行った場合で、IPフラグメントがブロックされたときに表示されます。エラーはブロックされたフラグメントごとに表示されます。
	Blocked - IP Source Routes	IPヘッダに始点経路制御オプションが設定されていることが原因で、パケットがブロックされたときに表示されます。
Firewall Setup	Blocked - State-table error	ファイアウォールによってステートテーブル（LAN側のパソコンやネットワーク機器間のセッション状態に関する情報）が調査または操作されている間に、エラーがあった場合に表示されます。パケットはブロックされます。
	Aborting configuration	ファイアウォールに関する設定がキャンセルされたときに表示されます。
	Configuration completed	ファイアウォールに関する設定が完了したときに表示されます。

WBM Login	Authentication Success	設定ページへのログインが成功したときに表示されます。
	Authentication Failure	設定ページへのログインが失敗したときに表示されます。
System Up/Down	The system is going DOWN for reboot	本製品を再起動するために終了したときに表示されます。
	The system is UP!	本製品が起動したときに表示されます。

■ログのクリア

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

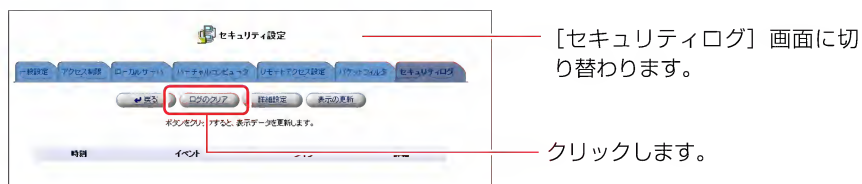
- 2 [セキュリティログ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

- 3** [ログのクリア] ボタンをクリックすると、画面に表示されてるログが消去されます。



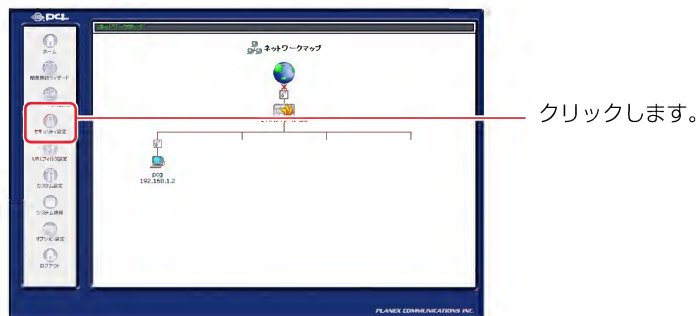
- 4** [戻る] ボタンをクリックします。

- 5** 以上で設定は終了します。

■ログの詳細設定

ここでは、ログの保存に関する設定について説明します。

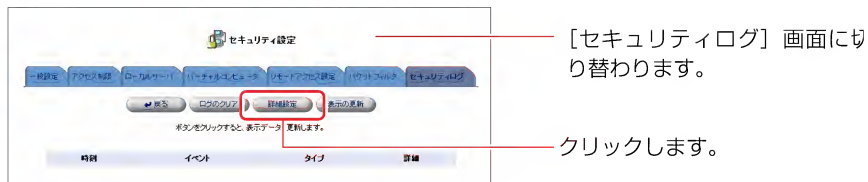
- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



- 2 [セキュリティログ] タブをクリックします。



3 [詳細設定] ボタンをクリックします。



4 [ログイベント] 欄から保存するログ内容を選択します。



[許可した接続]

LAN側からインターネットへの接続、インターネット側からLANへの接続のうちファイアウォールの通過を許可されたものがログに保存されます。

[拒否した接続]

LAN側からインターネットへの接続、インターネット側からLANへの接続のうちファイアウォールの通過を拒否されたものがログに保存されます。

[IPアドレスを詐称した接続]

LAN側からインターネットへの接続、インターネット側からLANへの接続のうち送信元IPアドレスを詐称してファイアウォールの通過を拒否されたものがログに保存されます。

5 「ログバッファ」欄からログ容量が一杯になったときの設定を選択します。



「ログバッファ」画面に
切り替わります。
選択します。

【ログ容量が一杯になったらログを停止する】

ログを保存するメモリが一杯になったときにログの保存を停止する場合は、チェックします。

ログを保存するメモリが一杯になったとき古いログを消去し、続けてログを保存する時はチェックを外します。

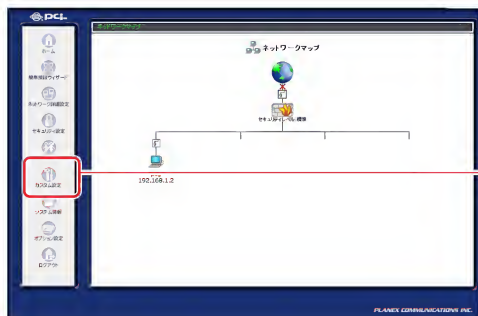
6 [OK] ボタンをクリックします。

7 以上で設定は終了します。

E-Mail 通知機能の設定

本製品は、システムや回線、ファイアウォールに何かしらの異常が発生した場合電子メールで管理者に通知することができます。

- 1 サイドバーから [カスタム設定] アイコンをクリックします。



クリックします。

- 2 [ユーザ] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 E-mail通知機能を設定するユーザの修正ボタンをクリックします。

[ユーザ] 画面に切り替わります。

修正 ボタンをクリックします。

4 [E-mailアドレス] 欄に、送信先の Mail アドレスを入力します。

[ユーザ設定] 画面に切り替わります。

入力します。

- 5** [システム通知レベル] 欄から通知する内容を選択します。
システム通知は、システム情報に関するメッセージを送信します。



ユーザ設定

一般設定

フルネーム: Administrator

ユーザ名 (大文字/小文字に注意): admin

新しいパスワード:

新しいパスワードの確認:

権限:

- ☒ 管理者権限
- ☐ PPTP リモートアクセス
- ☒ ファイルサーバからのファイルの読み込み
- ☒ ファイルサーバへのファイルの書き込み
- ☐ USBカメラ

E-Mail通知設定

SMTPメールサーバの設定

E-Mailアドレス:

システム通知レベル: **なし** (dropdown menu)

セキュリティ通知レベル:

OK キャンセル

入力します。

[エラー]

本製品が正しく動作していないなどの、致命的なエラーが発生した際にメッセージを送信します。

[警告]

注意を要するエラーが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

- 6 [セキュリティ通知レベル] 欄から通知する内容を選択します。
セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。



【エラー】

重大なセキュリティイベントが発生した際に、メッセージを送信します。

【警告】

注意を要するセキュリティイベントが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

【情報】

ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

- 7 本製品からメールを送信するための、SMTP メールサーバの設定をします。
[SMTP メールサーバの設定] をクリックします。



- 8** [SMTPメールサーバ] 欄にメールサーバのアドレスを入力します。
[送信元メールアドレス] 欄に送信元のメールアドレスを入力します。



SMTPメールサーバ

SMTPメールサーバ:

送信元メールアドレス:

入力します。

OK キャンセル

- 9** [OK] ボタンをクリックし、[ユーザ設定] 画面に戻ります。

- 10** [OK] ボタンをクリックします。

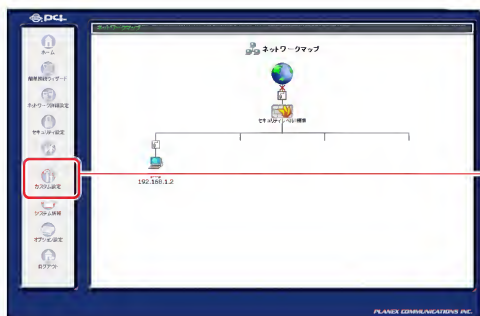
- 11** 以上で設定は終了です。

Syslogの設定

本製品には、システムや回線、ファイアウォールに何かしらの異常が発生した場合Syslogサーバにログを送信することができます。

ここでは、ログをSyslogサーバに送信するための設定を説明します。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

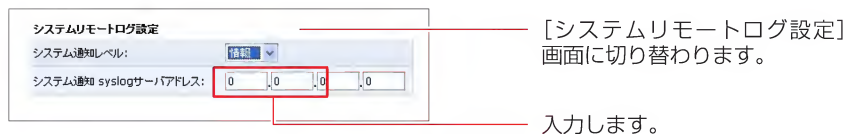
- 2 [システム設定]アイコンをクリックします。



「カスタム設定」画面に切り替わります。

クリックします。

- 3** [システム通知レベル] 欄から通知する内容を選択し、[システム通知 Syslog サーバアドレス] に syslog サーバのアドレスを入力します。



[エラー]

システムに関する重大なメッセージを送信します。

[警告]

システムに関する注意を要するメッセージを送信します。

警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。

情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

- 4** [セキュリティ通知レベル] 欄から通知する内容を選択し、[セキュリティ通知 syslog サーバアドレス] に Syslog サーバのアドレスを入力します。
セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。



[セキュリティリモートログ設定] 画面に切り替わります。

入力します。

[エラー]

重大なセキュリティイベントに関するメッセージを送信します。

[警告]

注意を要するセキュリティイベントに関するメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

- 5** [OK] ボタンをクリックします。

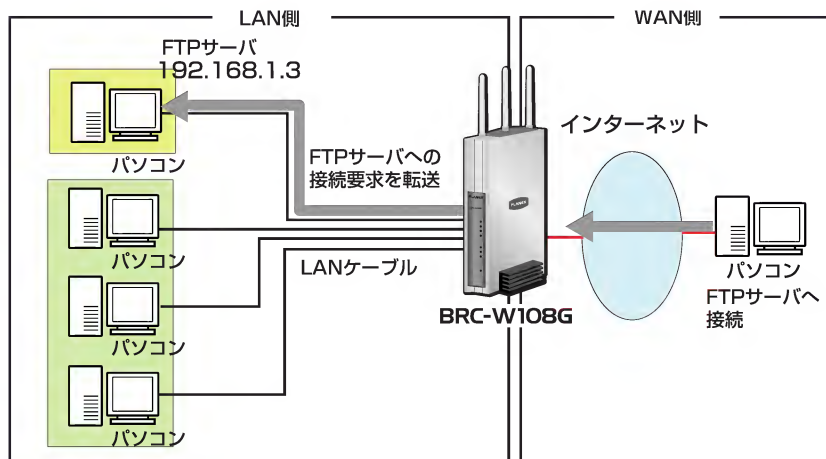
- 6** 以上で設定は終了です。

LAN側パソコンサーバ公開設定

ここでは、LAN側に設定したパソコンを公開するときに必要な設定について説明します。

ローカルサーバ設定

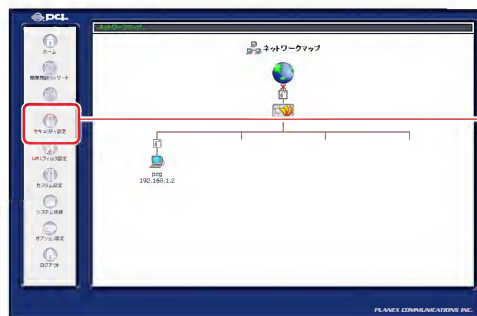
LAN側のサーバをインターネットに公開するときや、オンラインゲームやチャットなどのソフトウェアを使うときはローカルサーバ機能の設定を行います。本製品には、あらかじめインターネットで使われるサービスやアプリケーションが登録されており、簡単に設定することができます。



ローカルサーバの設定

ここでは、ローカルサーバの詳細な設定を行います。

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

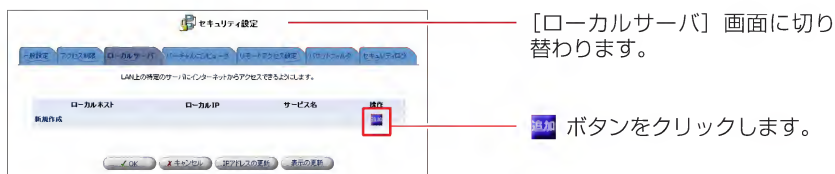
- 2 [ローカルサーバ]タブをクリックします。



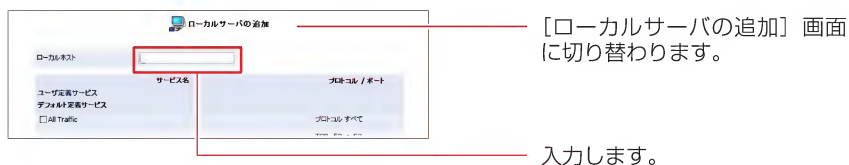
[セキュリティ設定] 画面に切り替わります。

クリックします。

3 [新規作成]欄から追加ボタンをクリックします。



4 [ローカルサーバの追加]画面が表示されます。 [ローカルホスト]欄にローカルサーバを設定するパソコンのIPアドレスを入力します。

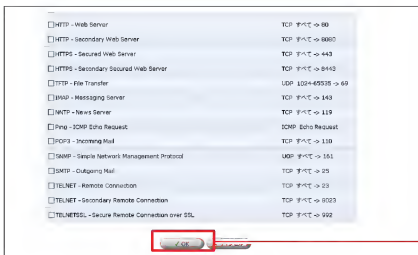


- 5** [デフォルト定義サービス]欄に本製品に既に登録されているサービスやアプリケーションが表示されます。インターネットに公開するサービスや、使用するアプリケーションを選択し、チェックします。



チェックします。

- 6** [OK]ボタンをクリックします。



クリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

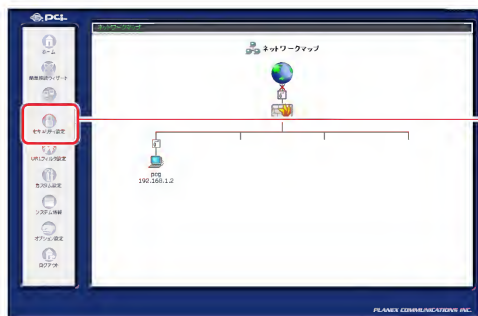
- 7** 以上で設定は終了です。

新規に作成したサービスでローカルサーバを設定する場合

■ユーザ定義サービスの新規作成

ここでは、本製品にあらかじめ登録されていないサービスを設定し、ローカルサーバを利用する方法について説明します。

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

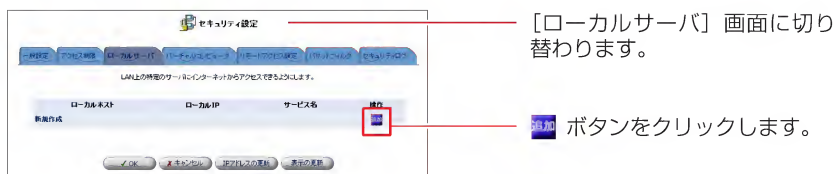
- 2 [ローカルサーバ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

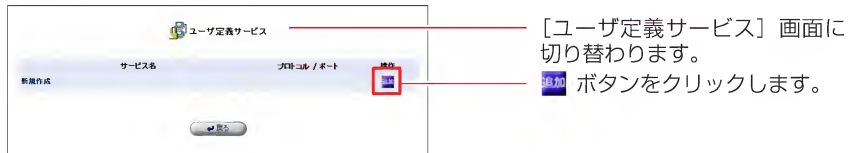
3 [新規作成]欄から追加ボタンをクリックします。



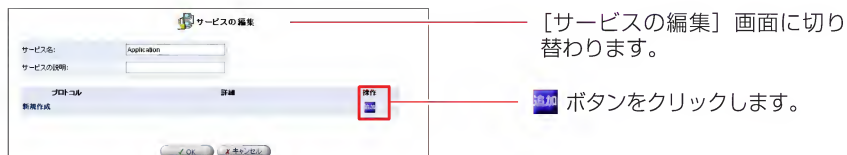
4 新規サービスを登録します。 [ユーザ定義サービス]をクリックします。



5 [ユーザ定義サービス]画面が表示されます。 [新規作成]欄から[追加]ボタンをクリックします。



6 [サービスの編集]画面が表示されます。 [新規作成]欄から[追加]ボタンをクリックします。



6 [プロトコル]欄から使用するプロトコルを選択し、ポート番号を入力します。

[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。その他を選択したときは、対象にするプロトコル番号を直接指定してください。

[発信元ポート/送信先ポート]

サービスやアプリケーションのポート番号を入力します。

すべて → 全てのポートを指定します。

1個を指定 → 1つのポート番号を指定します。

範囲指定 → ポート番号の範囲を指定します。

[ICMPメッセージ]

対象にするICMPメッセージを選択します。

7 [OK]ボタンをクリックします。



[サービスの編集] 画面に戻ります。

クリックします。

8 追加ボタンをクリックすることで、複数のポートを指定することもできます。

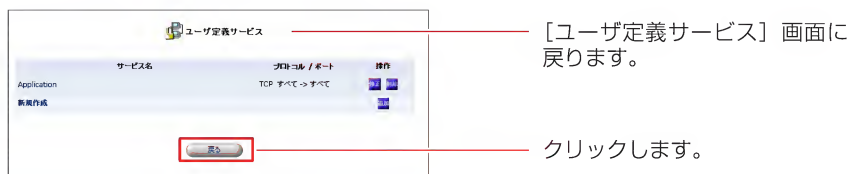


入力します。

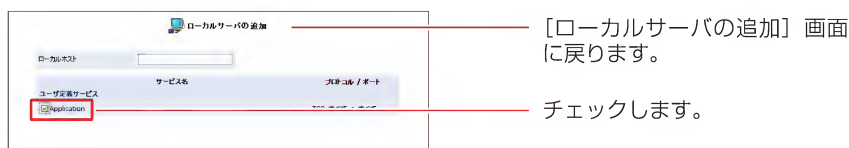
追加 ボタンをクリックします。

9 全ての設定が終了しましたら、[サービス名]欄に任意の名前を入力し、[OK]ボタンをクリックします。

- 10** [ユーザ定義サービス]の画面に戻ります。
[サービス名]欄に作成したユーザ定義サービスが表示されてるのを確認
します。[戻る]ボタンをクリックします。



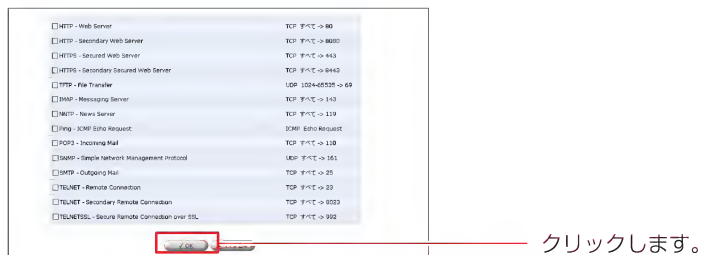
- 11** [ローカルサーバの追加]の画面に戻ります。
[ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されてるの
を確認し、チェックします。



- 12** ローカルサーバ機能を使用するパソコンの設定を行います。
[ローカルホスト]欄にローカルサーバ機能を使用するパソコンのIPアドレス
を入力します。



- 13** [OK]ボタンをクリックします。



※[OK]ボタンは画面の下の方にあります。スクロールして表示させてください。

- 14** [ローカルサーバ]の画面に戻ります。ローカルサーバで使用するサービスとパソコンのIPアドレスが表示されます。



[ローカルサーバ] 画面に戻ります。

表示されます。

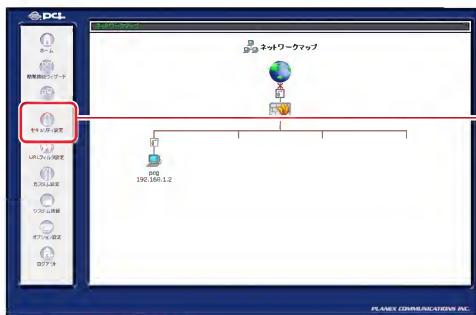
- 15** [OK]ボタンをクリックします。

- 16** 以上で設定は終了です。

■ユーザ定義サービスの修正

ここでは、既に作成したユーザ定義サービスを修正する方法について説明します。

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

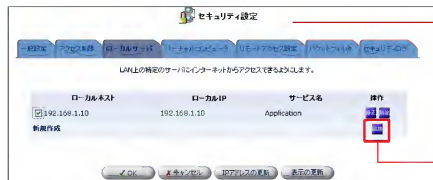
- 2 [ローカルサーバ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

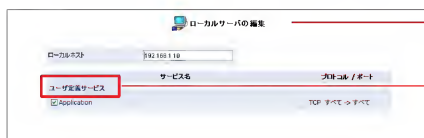
- 3 設定を変更するパソコンの修正ボタンをクリックします。



[ローカルサーバ] 画面に切り替わります。

修正 ボタンをクリックします。

- 4** [ローカルサーバの編集]画面が表示されます。
[ユーザー定義サービス]をクリックします。



[ローカルサーバの編集] 画面に切り替わります。
クリックします。

- 5** [ユーザ定義サービス]の画面が表示されます。設定を変更したいサービスの修正ボタンをクリックします。



[サービスの編集] 画面に切り替わります。
修正 ボタンをクリックします。

- 6** [サービスの編集]の画面が表示されます。設定を変更したいプロトコルの修正ボタンをクリックします。



[サービスの編集] 画面に切り替わります。
修正 ボタンをクリックします。

- 7** [サービスの編集]の画面が表示されます。設定を変更したい項目を修正し、[OK]ボタンをクリックします。



[サービスの編集] 画面に切り替わります。
修正します。
クリックします。

8 [OK]ボタンをクリックします。



[サービスの編集] 画面に切り替わります。

クリックします。

9 [ユーザ定義サービス]画面に戻ります。 [戻る]ボタンをクリックします。



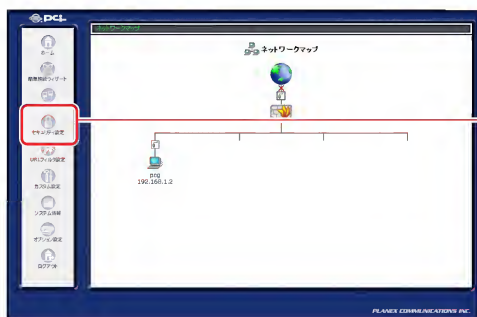
[サービスの編集] 画面に切り替わります。

クリックします。

10 以上で設定は終了です。

■ユーザ定義サービスの削除

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

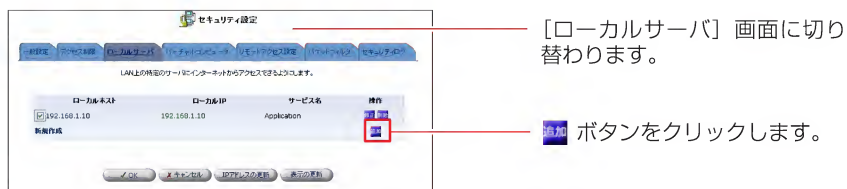
- 2 [ローカルサーバ]タブをクリックします。



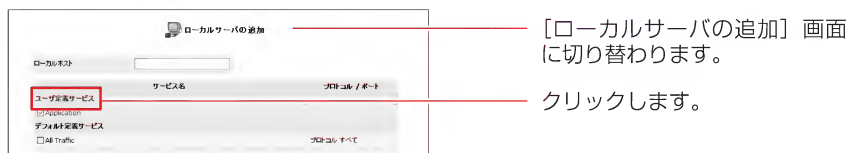
[セキュリティ設定] 画面に切り替わります。

クリックします。

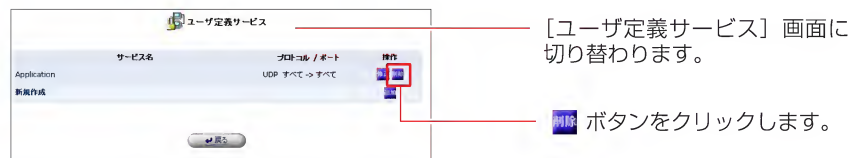
3 [新規作成]欄から追加ボタンをクリックします。



4 [ユーザ定義サービス]をクリックします。



5 [ユーザ定義サービス]の画面が表示されます。削除したいサービスの削除ボタンをクリックします。

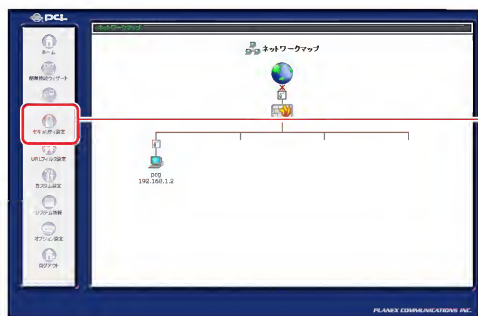


6 [戻る]ボタンをクリックします。

7 以上で設定は終了です。

設定したローカルサーバの修正

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

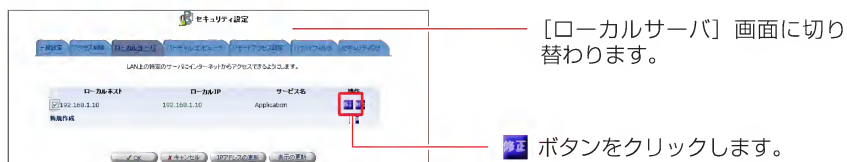
- 2 [ローカルサーバ]タブをクリックします。



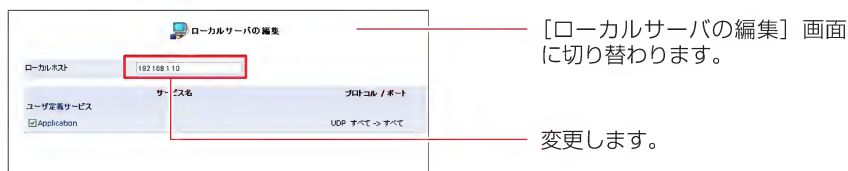
[セキュリティ設定] 画面に切り替わります。

クリックします。

3 設定を変更したいパソコンの修正ボタンをクリックします。



4 『ローカルサーバの編集』画面が表示されます。 使用するサービスまたはパソコンのIPアドレスを変更できます。

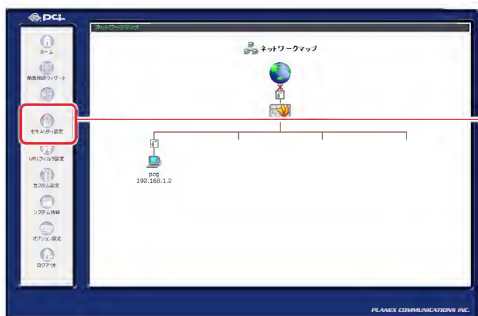


5 [OK]ボタンをクリックします。

6 以上で設定は終了です。

ローカルサーバの有効/無効の切替

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

- 2 [ローカルサーバ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

- 3 [ローカルホスト]欄からサービスを無効にしたいIPアドレスのチェックを外します。



[ローカルサーバ] 画面に切り替わります。

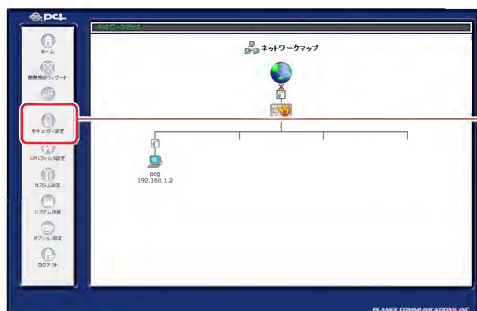
チェックを外します。

4 [OK] ボタンをクリックします。

5 以上で設定は終了です。

設定したローカルサーバの削除

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

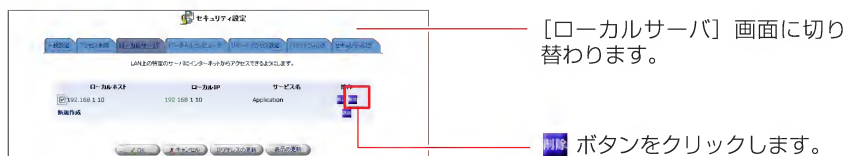
- 2 [ローカルサーバ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

3 設定を削除したいサービスの削除ボタンをクリックします。



4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

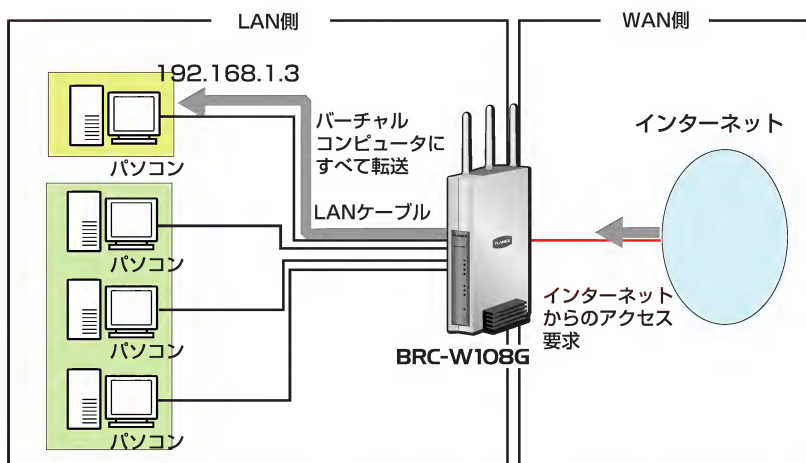
バーチャルコンピュータの設定

バーチャルコンピュータ機能を使用すると、LAN側にある1台のパソコンをインターネット上に公開できます。次のようなときに、バーチャルコンピュータを指定します。

- ・[ローカルサーバ]機能のリストにはないオンラインゲームやビデオ会議用のソフトウェアで、使用するポートなどの情報が公開されていない場合。
- ・セキュリティの制限無しに、1台のパソコンで全てのサービスをインターネットに公開する場合。

！ ご注意

- ・バーチャルコンピュータとして、複数のパソコンを設定することはできません。
- ・バーチャルコンピュータとして設定したパソコンは、ファイアウォールで保護されていないため、外部から攻撃を受ける恐れがあります。
- ・ローカルサーバ機能とバーチャルコンピュータ機能を同時に設定しているときは、ローカルサーバの設定が優先されます。
- ・DMZ（ポート）機能とバーチャルコンピュータ機能を同時に設定することはできません。



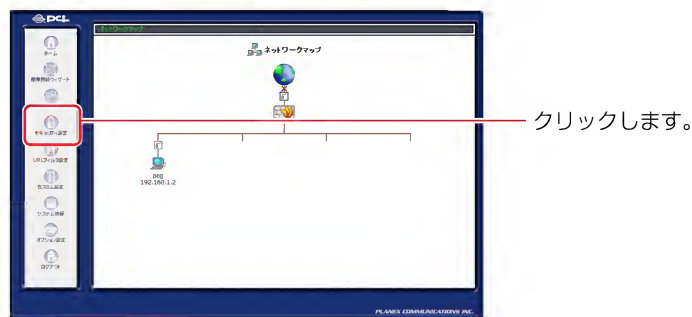
インターネットからLAN側へのアクセス要求を受け取ると、本製品は[ローカルサーバ]機能で登録されてる宛先を除き、すべてバーチャルコンピュータへその要求を転送します。

LAN側のパソコンをバーチャルコンピュータに設定する

ここでは、LAN側のパソコンをインターネットに公開するためのバーチャルコンピュータの設定について説明します。

■ バーチャルコンピュータ設定

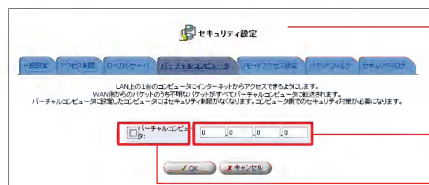
- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



- 2 [バーチャルコンピュータ]タブをクリックします。



- 3** [バーチャルコンピュータ IPアドレス]欄にチェックを付け、バーチャルコンピュータにするパソコンのIPアドレスを入力します。



[バーチャルコンピュータ] 画面に切り替わります。

入力します。

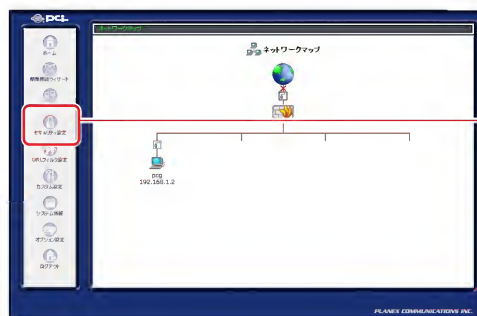
チェックします。

- 4** [OK]ボタンをクリックします。

- 5** 以上で設定は終了です。

■ バーチャルコンピュータの有効/無効の切替

- 1 サイドバーから[セキュリティ設定]アイコンをクリックします。



クリックします。

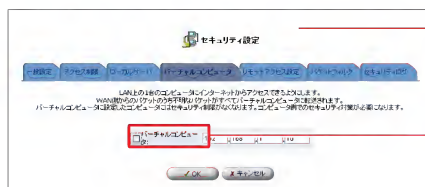
- 2 [バーチャルコンピュータ]タブをクリックします。



「セキュリティ設定」画面に切り替わります。

クリックします。

3 [バーチャルコンピュータIPアドレス]欄からチェックを外します。



[バーチャルコンピュータ] 画面に切り替わります。

チェックを外します。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

ダイナミック DNS の設定

WEBサーバなどをインターネットに公開するときは、固定のグローバルIPアドレスが本製品に割り当てられている必要があります。しかし、インターネットに常時接続していても切断、再接続の際に動的にIPアドレスが変わってしまう場合があります。

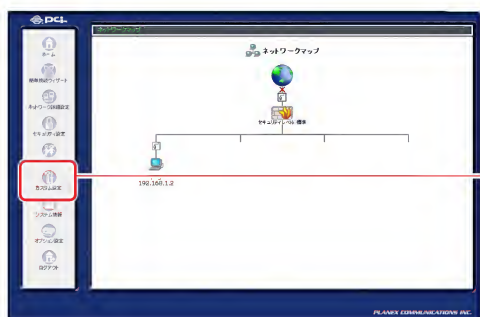
ダイナミックDNSを使用すると、本製品のIPアドレスをダイナミックDNSサーバに一定間隔で通知することで、IPアドレスが変わった場合でも固定のホスト名が使用できます。

ご注意

- ・ 本製品は「www.dyndns.org」ダイナミックDNSサービスに対応しています。本製品のダイナミックDNSの設定を行う前に、「www.dyndns.org」にアクセスし、ユーザ名、パスワード、ホスト名の登録を行ってください。
- ・ 「www.dyndns.org」は、無償のサービスです（2005年3月現在）。また、プロバイダによっては本設定を使わなくても、ダイナミックDNSを実現することが出来る場合があります。詳しくは、プロバイダにお問い合わせ下さい。

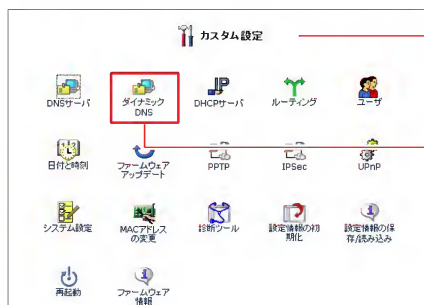
ダイナミックDNSの設定

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

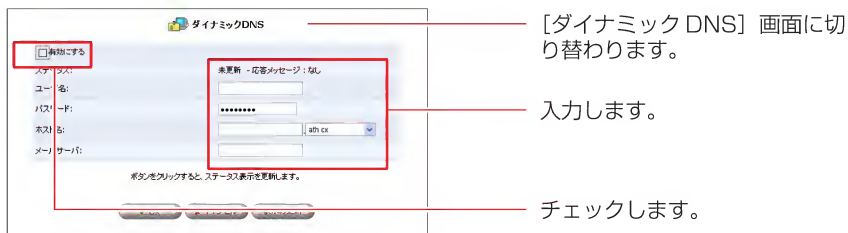
- 2 [ダイナミックDNS]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

- 3** [ダイナミック DNS]の画面が表示されます。
[有効にする]欄にチェックを付け、ダイナミック DNS サービスに登録した内容をもとに各項目を入力します。



[ステータス]

現在の更新情報が表示されます。

[ユーザ名]

ダイナミック DNS サービスに登録されているユーザ名を入力します。

[パスワード]

ダイナミック DNS サービスに登録されているユーザパスワードを入力します。

[ホスト名]

テキスト欄に登録したホスト名とドメイン名を入力してください。

[メールサーバ]

メールサーバを登録したい場合は、メールサーバのホスト名を入力します。

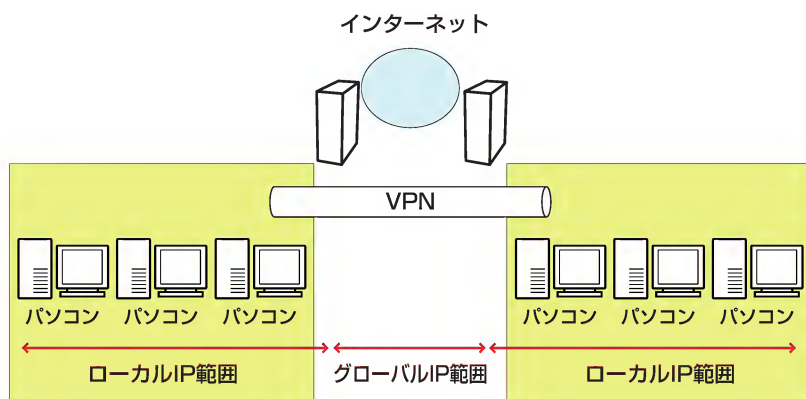
- 4** [OK]ボタンをクリックします。

- 5** 以上で設定は終了です。
設定が完了するとダイナミック DNS サーバへ本製品が取得している IP アドレスを定期的に通知するようになります。

VPNの設定

VPN (Virtual Private Network) は、データのカプセル化や暗号化などのセキュリティ技術を使って、インターネットを仮想的に、専用線で接続したWANのように利用する技術です。VPNを構築するためには、PPTP (Point to Point Tunneling Protocol) やIPSec (IP Security) などのプロトコルが用いられます。ここでは、PPTPとIPSecによるVPN接続の方法について説明します。

本製品は、PPTPサーバとPPTPクライアントおよびIPSecの機能を搭載しているため、パソコンにVPN用のソフトウェアを導入する必要もなく、強固なセキュリティ機能をもつVPNを構築することができます。



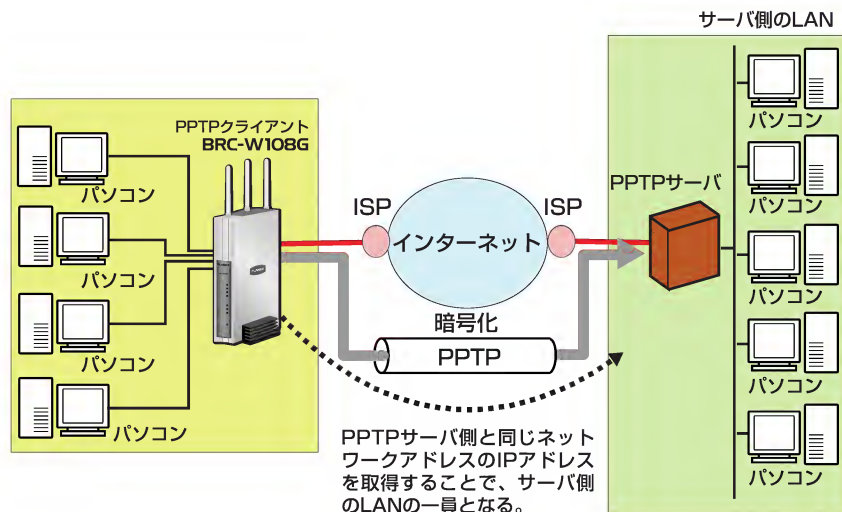
VPNを構築するには、簡単接続ウィザードによる設定をした後、ネットワーク詳細設定によって、詳細な設定が可能です。次ページの簡単接続ウィザードから設定を進めてください。なお、すでに簡単接続ウィザードによるVPN接続設定が終わっている場合は、「ネットワーク詳細設定による設定」に進んでください。

簡単接続ウィザードによる設定

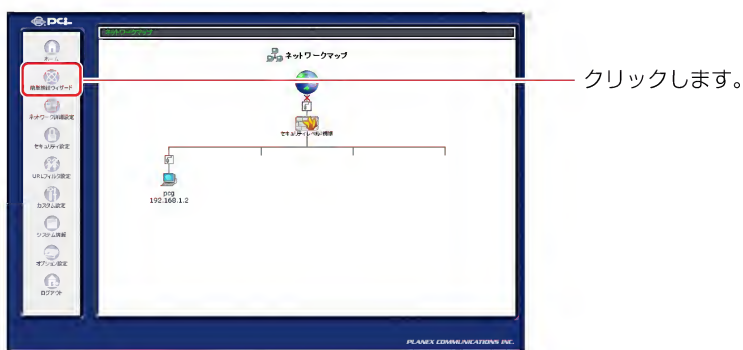
ここでは、簡単接続ウィザードを使いVPNを構築する方法について説明します。本製品はPPTPサーバ、PPTPクライアント、IPSecに対応しています。ご利用する環境に合わせて設定を進めてください。

■ PPTPクライアントの設定

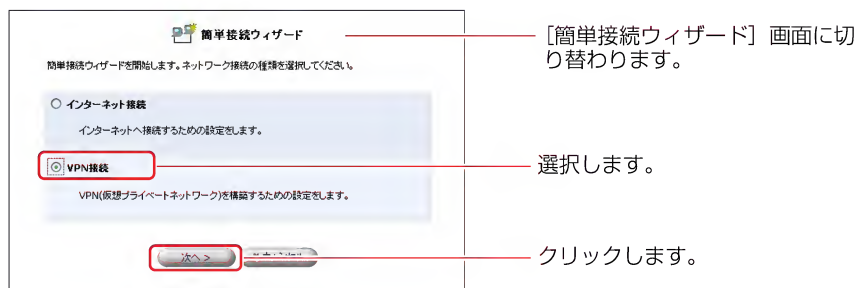
本製品をPPTPクライアントとして使用する場合の設定について説明します。



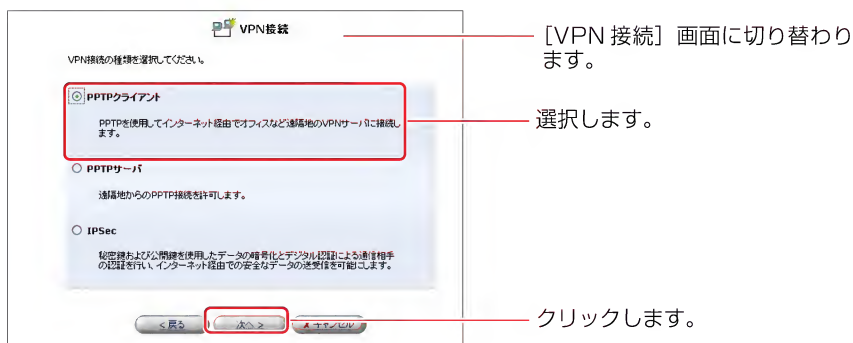
1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。



2 [VPN接続]を選択し、[次へ]ボタンをクリックします。



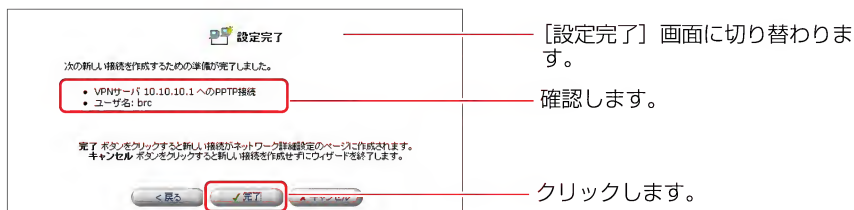
3 [PPTPクライアント]を選択し、[次へ]ボタンをクリックします



- 4** リモートアクセスするサーバの設定に従い、PPTP接続の設定を行います。
[接続先のホスト名またはIPアドレス]に接続するPPTPサーバのIPアドレスを入力し、[接続ユーザ名]、[接続パスワード]に接続する時のユーザ名とパスワードを入力します。
[次へ]ボタンをクリックします。

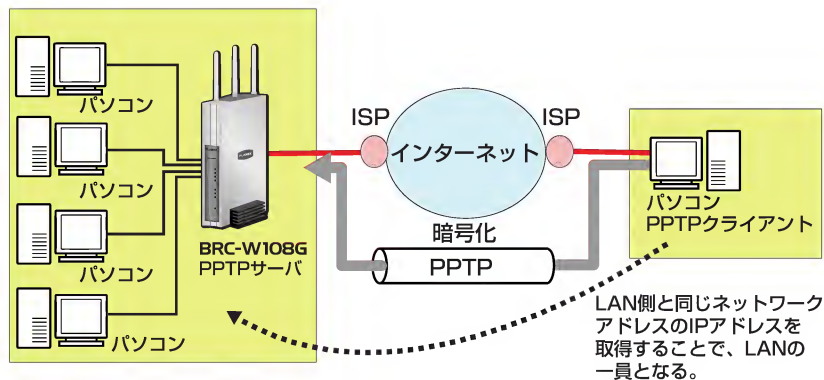


- 5** [接続完了]画面が表示されます。
PPTP 接続するサーバ名またはIPアドレスを確認し、[完了]ボタンをクリックします。

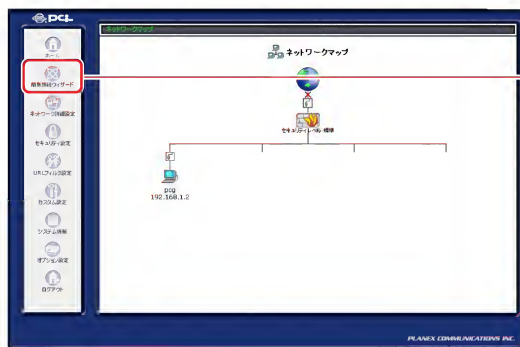


■ PPTP サーバの設定

本製品をPPTPサーバとして使用する場合の設定について説明します。

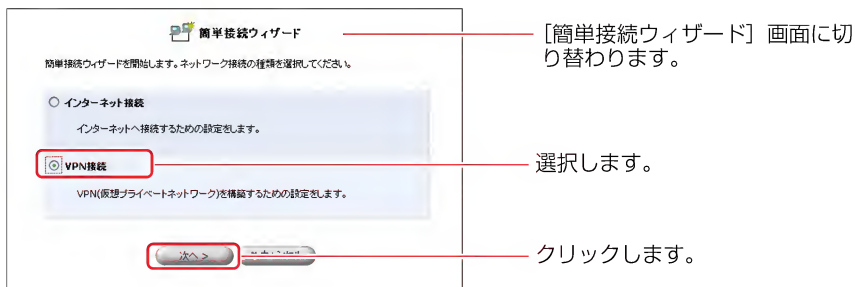


- 1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

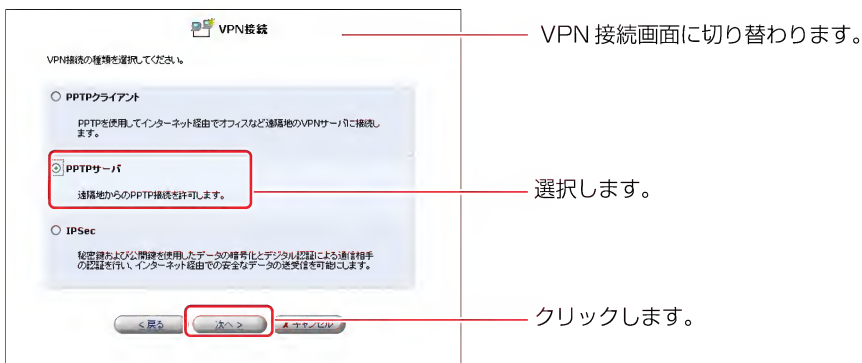


クリックします。

2 [VPN接続]を選択し、[次へ]ボタンをクリックします。



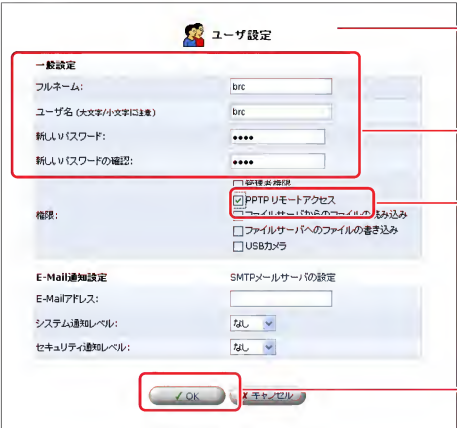
3 [PPTPサーバ]を選択し、[次へ]ボタンをクリックします。



4 PPTPサーバにアクセスを許可する為のユーザ設定を行います。



- 5 [一般設定]欄のフルネーム、ユーザ名、新しいパスワード、新しいパスワードの確認に登録するユーザの設定を入力し、[権限]欄からPPTPリモートアクセスにチェックをつけます。




[ユーザ設定] 画面に切り替わります。

入力します。

チェックします。

クリックします。

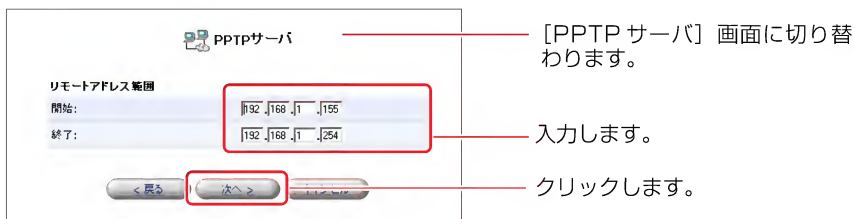
- 6 ユーザの追加または修正、削除が終わると[ユーザ]画面に戻りますので、[次へ]ボタンをクリックします。



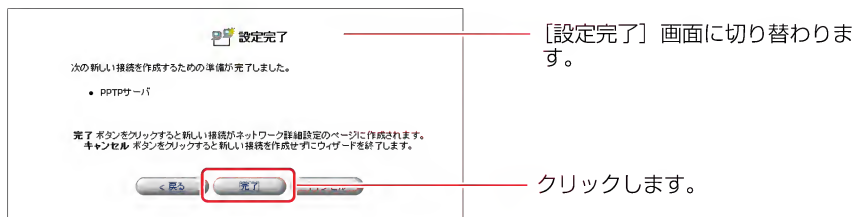
[ユーザ] 画面に戻ります。

クリックします。

- 7** PPTPクライアントのリモートアドレスを入力します。
PPTPサーバにリモートアクセスするユーザに割り当てるIPアドレスの範囲を入力し、[次へ]ボタンをクリックします。



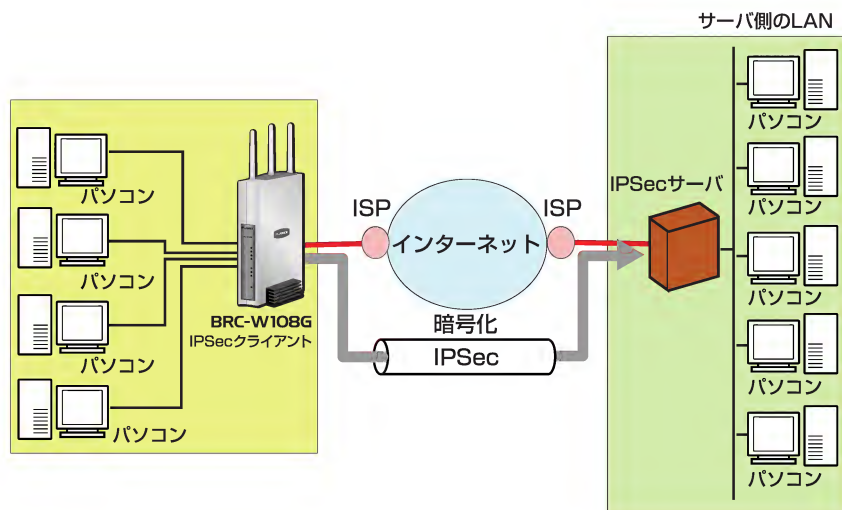
- 8** [設定完了]画面が表示されます。
[完了]ボタンをクリックします。



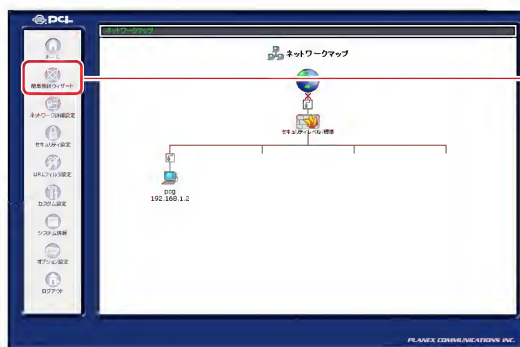
インターネットに接続されている場合、PPTPクライアントの設定が完了すると、自動的にPPTPサーバへ接続を行います。

■ IPsecの設定

本製品を使いIPsecによるVPN接続を行う場合の設定について説明します。

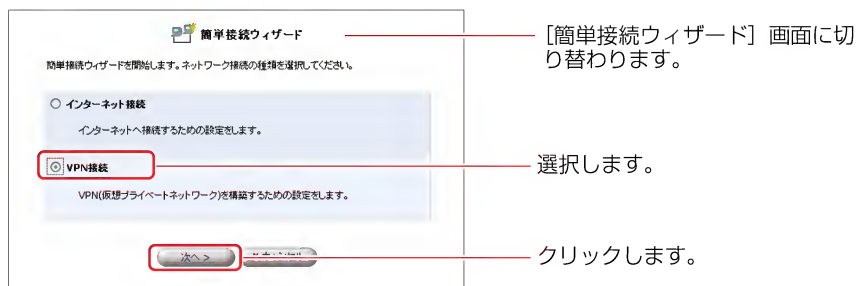


- 1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

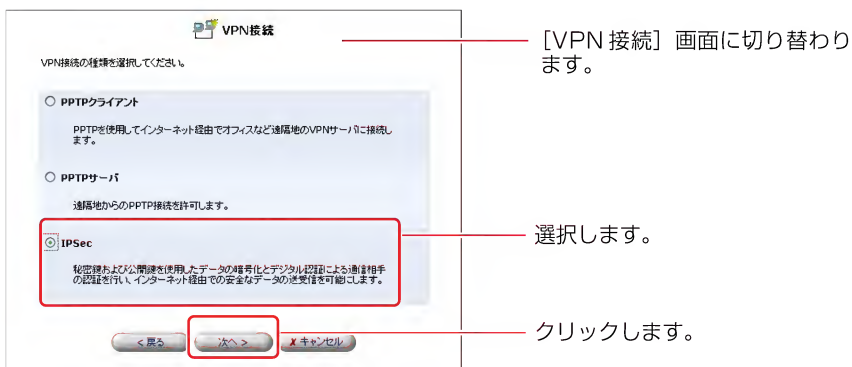


クリックします。

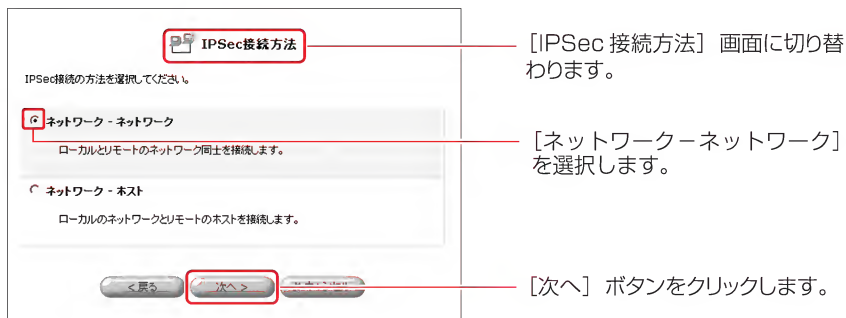
2 [VPN接続]を選択し、[次へ]ボタンをクリックします。



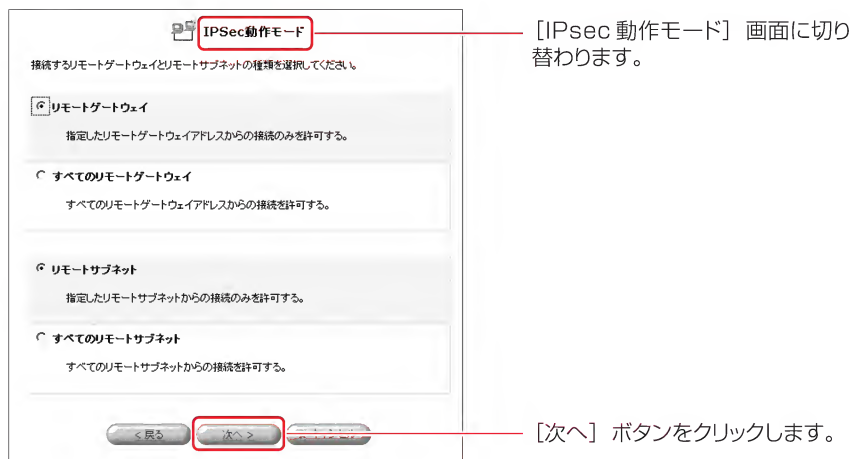
3 [IPSec]を選択し、[次へ]ボタンをクリックします。



4 [ネットワーク - ネットワーク]を選択し、[次へ]ボタンをクリックします。



- 5 [IPSec動作モード]を設定します。接続するリモートゲートウェイとリモートサブネットの種類を選択し、[次へ]ボタンをクリックします。



[リモートゲートウェイ]

指定したリモートゲートウェイアドレスからの接続のみを許可するときに選択します。

[すべてのリモートゲートウェイ]

すべてのリモートゲートウェイアドレスからの接続を許可するときに選択します。


[リモートサブネット]

指定したリモートサブネットからの接続のみを許可するときに選択します。

[すべてのリモートサブネット]

すべてのリモートサブネットからの接続を許可するときに選択します。

- 6 接続するIPSecの情報を入力し、[次へ]ボタンをクリックします。
「IPSec動作モード」の選択によって入力する項目は異なります。



The screenshot shows the 'IPSec' configuration window. At the top, it says 'IPSec' with a small icon. Below that, it says 'IPSec接続の設定をします。' (Configure IPSec connection). There are four input fields: '接続先のホスト名またはIPアドレス:' (Host name or IP address of the connection destination), 'リモートサブネット:' (Remote subnet), 'リモートサブネットアドレス:' (Remote subnet address), and 'リモートサブネットマスク:' (Remote subnet mask). Each of these four fields is highlighted with a red box. Below them is a field for '共通鍵(Shared Secret):' (Shared secret). At the bottom, there are three buttons: '< 戻る' (Back), '次へ >' (Next), and '完了' (Finish). The '次へ >' button is highlighted with a red box.

[IP Sec] 画面に切り替わります。

入力します。

クリックします。

【接続先のホスト名またはIPアドレス】

IPSecで接続する相手側のIPアドレスを入力します。

【リモートサブネットアドレス】

IPSecで接続する相手側のネットワークアドレスを入力します。

【リモートサブネットマスク】

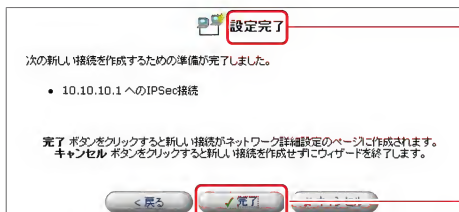
IPSecで接続する相手側のサブネットマスクを入力します。

【共通鍵】

IPSec間で認証を行うときに使う事前共有鍵を入力します。

鍵の値は両方のルータで同じ値を入力します。

- 7 【設定完了】画面が表示されます。[完了]ボタンをクリックします。



The screenshot shows the '設定完了' (Setup Complete) screen. At the top, it says '設定完了' with a small icon. Below that, it says '次の新しい接続を作成するための準備が完了しました。' (Preparation for creating the next new connection is complete). There is a bullet point: '10.10.10.1 へのIPSec接続' (IPSec connection to 10.10.10.1). Below that, it says '完了 ボタンをクリックすると新しい接続がネットワーク設定のページに作成されます。' (Clicking the Finish button will create a new connection on the network settings page.) and 'キャンセル ボタンをクリックすると新しい接続を作成せずにフィニッシュを終了します。' (Clicking the Cancel button will finish without creating a new connection). At the bottom, there are three buttons: '< 戻る' (Back), '完了' (Finish), and 'キャンセル' (Cancel). The '完了' button is highlighted with a red box.

【設定完了】画面に切り替わります。

【完了】ボタンをクリックします。
【完了】ボタンは続けてクリックせずに、1回のみクリックしてください。

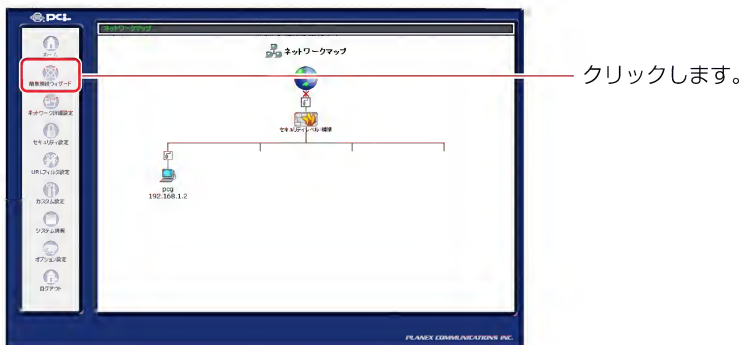
ネットワーク詳細設定による設定

PPTPクライアントやサーバに関する詳細な設定と、IPSecの詳細設定について説明します。

VPNの詳細な設定をするためには、あらかじめ「簡単接続ウィザード」による設定を終了しておく必要があります。

■ PPTPクライアントの詳細設定

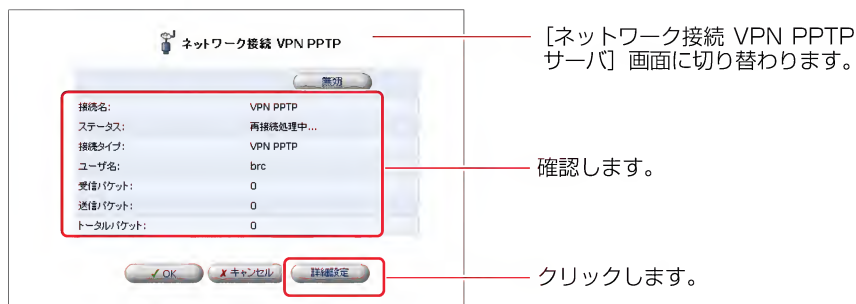
- 1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします。



- 2 [ネットワーク詳細設定] 画面が表示されます。詳細な設定を行うVPN PPTP接続の修正ボタンをクリックします。



- 3 [ネットワーク詳細設定 VPN PPTP] 画面が表示されます。接続名、ステータス、ユーザ名等が表示されていますので、確認して[詳細設定] ボタンをクリックします。



- 4 [詳細設定VPN PPTP] 画面が表示されます。PPTPサーバ管理者の通知に従って、基本設定、PPP、PPP 認証、PPP 暗号化、IP の設定方法などを設定します。

◎基本設定、PPP、PPP 認証の設定

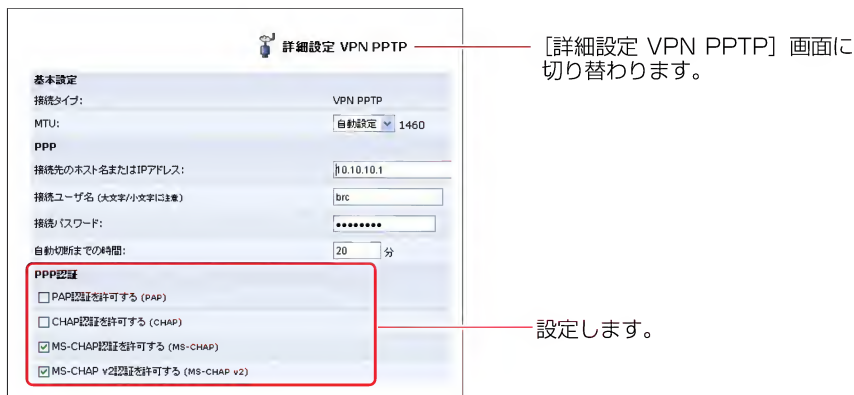
[PPP]

接続先のホスト名またはIPアドレス、接続ユーザ名、接続パスワードには、簡単接続ウィザードで設定した内容が表示されています。変更する必要がある項目を修正します。

自動切断までの時間は、PPTPによる通信が中断したときに接続を切断するまでの時間を分単位で入力します。

[PPP 認証設定]

ユーザ認証のためのプロトコルを選択します。PPP 暗号化で「暗号化を許可する」場合は、MS-CHAP またはMS-CHAP v2 を選択します。



◎ PPP 暗号化、IP 設定

パケットの暗号化に関する設定を行います。

[PPP 暗号化]

- ・ 暗号化を必ず要求する：
暗号化通信を要求するときにチェックします。サーバが拒否すると PPTP 通信は確立されません。
- ・ 暗号化を許可する：
暗号化に MPPE (Microsoft Point-to-Point Encryption) を使用します。40bit のキーで暗号化するか、128bit のキーを使うかで、MPPE-40 か MPPE-128 を選択します。
- ・ MPPE 暗号化モード：
暗号化のモード (Stateless または Stateful) を選択します。Stateless はパケットごとに暗号化キーを変更するので、通信の安全性は高くなります。Stateful は複数のパケット単位で暗号化キーを変更します。
暗号化を許可する場合は、上の PPP 認証で、MS-CHAP または、MS-CHAP v2 が選択されていることを確認してください。

[IP 設定]

IP アドレスを固定にするか、自動取得するかを選択します。

[サブネットマスクを置き換える] は、固定のサブネットマスクを利用するときにチェックし、そのときのサブネットマスクを指定します。

[DNS サーバ]

DNS サーバアドレスを自動取得するのか、固定設定にするのかを選択します。固定にする場合は、プライマリとセカンダリ DNS サーバの IP アドレスを指定します。
なお、[DNS サーバ] をクリックすると、[カスタム設定] で [DNS サーバ] を選んだ状態になります。

[デバイスメトリック]

メトリックの値を入力します。

！ ご注意

必ず [NAPT] は有効の状態でお使いください。

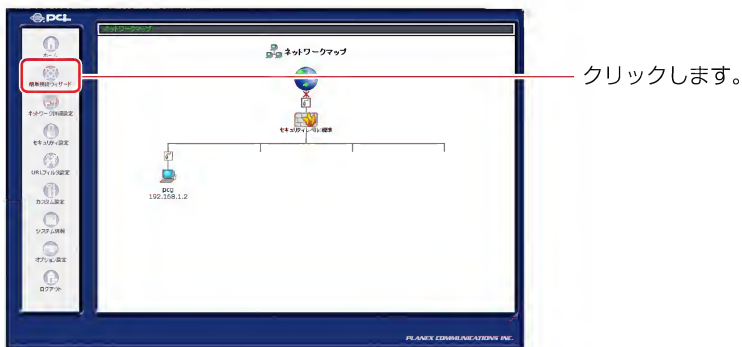
設定します。

- 5 [OK] ボタンをクリックすると設定が有効になり、[ネットワーク接続 VPN PPTP] 画面に戻ります。

■ PPTPクライアントの削除

ここでは、既に登録してあるPPTPクライアント接続を削除する場合について説明します。

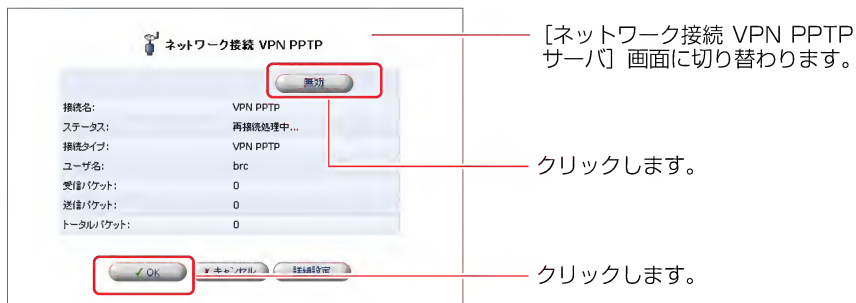
1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします



2 [接続名]欄から削除するVPN PPTP接続の[修正]ボタンをクリックします。



- 3** 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。



- 4** [接続名]欄から削除するVPN PPTP接続の[削除]ボタンをクリックします。

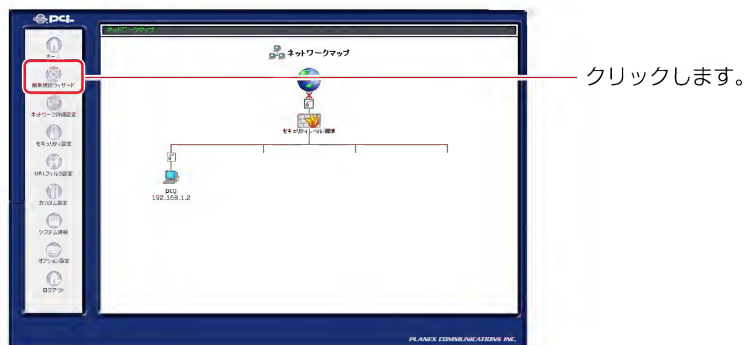


- 5** [戻る]ボタンをクリックします。

- 6** 以上で設定は終了です。

■ PPTP サーバの詳細設定

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします

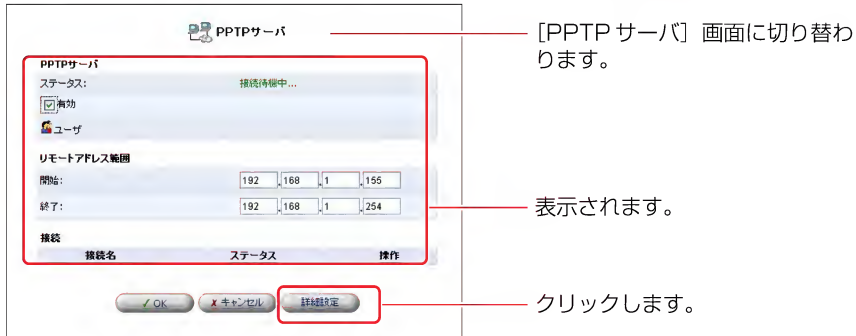


2 [ネットワーク詳細設定] 画面が表示されます。詳細な設定を行う VPN PPTP サーバ接続の修正ボタンをクリックします。

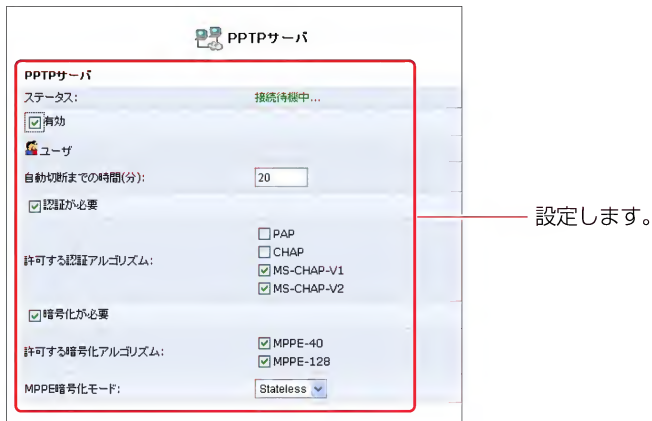


※ PPTPサーバを削除する場合は、修正ボタンをクリックし、[PPTPサーバ] 画面の [有効] 欄からチェックを外します。

- 3** [PPTPサーバ] 画面が表示されます。
[詳細設定] ボタンをクリックします。
なお、ここでユーザの編集、PPTPクライアントの接続設定も可能です。



- 4** [PPTPサーバ] 画面が表示されます。PPTPサーバの詳細な設定を行います。



[ステータス]

PPTPサーバの接続状況を表示します。

[有効]

PPTPサーバを有効にするときにチェックします。このチェックをはずすと、PPTPサーバとして動作しなくなり、接続状況にも反映されなくなり、また詳細設定の画面からも削除されます。

[ユーザ]

クリックすると、ユーザの設定を行うことができます。

【自動切断までの時間】

PPTPによる通信が中断したときに、接続を切断するまでの時間を分単位で入力します。

【ユーザセキュリティ】

PPTPを使用した通信での認証と暗号化について設定します。

- ・ 認証が必要：
PPTPクライアントが接続するときに、ユーザ認証を必要とするときにチェックします。接続テストなど特別な場合を除いて必ずチェックを入れてください。
- ・ 暗号化が必要：
PPTPクライアントが接続するときに、暗号化通信を要求する場合にチェックします。

【許可する認証アルゴリズム】

ユーザセキュリティで認証が必要にチェックをした場合、認証のアルゴリズムをPAP、CHAP、MS-CHAP-v1、MS-CHAP-v2 から選択します。暗号化をする場合は、MS-CHAP-v1かMS-CHAP-v2をチェックしてください

【許可する暗号化アルゴリズム】

ユーザセキュリティで暗号化が必要にチェックをした場合、暗号化アルゴリズムをMPPE-40 と MPPE-128 から選択します。

【MPPE 暗号化モード】

暗号化のモード (Stateless または Stateful) を選択します。

- ・ Stateless：
パケットごとに暗号化キーを変更するので、通信の安全性は高くなります。
- ・ Stateful：
複数のパケット単位で暗号化キーを変更します。

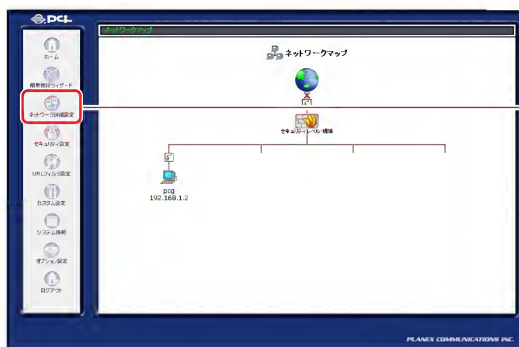
- 5** [簡単接続ウィザード] で設定した、リモートアドレス、クライアントとして動作する場合のPPTPクライアントの設定が表示されます。クリックし修正することが可能です。



- 6** [OK] ボタンをクリックすると、設定が有効になりネットワーク詳細設定画面に戻ります。[基本設定] ボタンをクリックすると、PPTPサーバの最初の画面に戻ります。

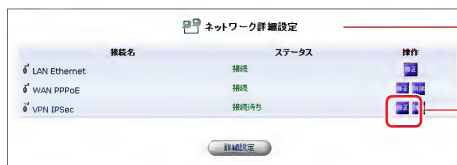
■ IPSecの詳細設定

- 1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします



クリックします。

- 2 [ネットワーク詳細設定]画面が表示されます。詳細な設定を行うVPN IPSec接続の修正ボタンをクリックします。



[ネットワーク詳細設定]画面に切り替わります。

修正ボタンをクリックします。

- 3 [ネットワーク接続 VPN IPSec]画面が表示されます。[詳細設定]ボタンをクリックします。



[ネットワーク接続 VPN IPSec]画面に切り替わります。

クリックします。

4 「詳細設定 VPN IPSec」画面が表示されます。

「詳細設定 VPN IPSec」画面に切り替わります。

ここで次の項目を設定します。

基本設定

【MTU】

MTUを設定します。

【接続先のホスト名またはIPアドレス】

簡単接続ウィザードで設定した接続先が表示されています。必要であれば修正します。

【ローカルサブネット】

本製品のLAN側のサブネットアドレス、サブネットマスクを設定します。

【リモートサブネット】

接続先のサブネットアドレスとサブネットマスクを入力します。

【データ圧縮】

データ圧縮をするときにチェックします。

【鍵交換方式】

暗号化アルゴリズムや鍵交換のためのSAの合意をとる方式を選択します。

・自動：

IKE (Internet Key Exchange) を使って、SAの合意を通信時に自動的に行う場合に選択します。通常は、自動に設定しておきます。

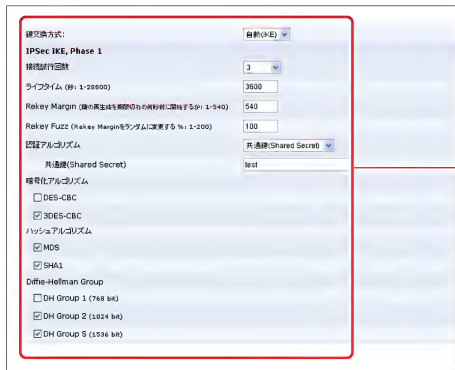
・手動：

SAの合意をあらかじめ手動で設定しておく場合に選択します。画面が手動用に切り替わります。

❗ ご注意

必ず手動モードは「トンネリング」の状態でお使いください。

- 5 鍵交換方式を自動に設定します。
- 鍵交換方式を[自動]に設定した場合、次の2つのフェーズの設定を行います。
- まず、IPSec IKE, Phase 1の設定をします。



The screenshot shows the configuration window for IPSec IKE, Phase 1. The 'Key Exchange Method' is set to 'Automatic'. The 'Authentication Algorithm' is set to 'Common Key (Shared Secret)'. The 'Encryption Algorithm' is set to 'DES-CBC'. The 'Hash Algorithm' is set to 'MD5'. The 'Diffie-Hellman Group' is set to 'DH Group 2 (1024 bit)'. The 'Lifetime' is set to 3600. The 'Rekey Margin' is set to 540. The 'Rekey Fuzz' is set to 100. The 'Authentication Algorithm' is set to 'Common Key (Shared Secret)'. The 'Encryption Algorithm' is set to 'DES-CBC'. The 'Hash Algorithm' is set to 'MD5'. The 'Diffie-Hellman Group' is set to 'DH Group 2 (1024 bit)'.

設定します。

IPSec IKE, Phase 1

[接続試行回数]

ネゴシエーションの試行回数を設定します。

[ライフタイム]

鍵の有効期限を秒単位で設定します。

[Rekey Margin]

Rekey (鍵の再生成) を期限切れの何秒前に開始するかを設定します。

[Rekey Fuzz]

Rekey Marginをランダムに変更するパーセンテージを設定します。

[認証アルゴリズム]

認証の方式を選択します。

- ・ 共通鍵方式：
共通鍵方式を選択する場合は、事前共有キーの文字列を入力します。
(かんたん設定ウィザードで入力した鍵が表示されます。)
- ・ 公開鍵方式：
公開鍵方式を使用する場合に、キーの文字列を入力します。

[暗号化アルゴリズム]

使用する暗号化アルゴリズムをチェックします。

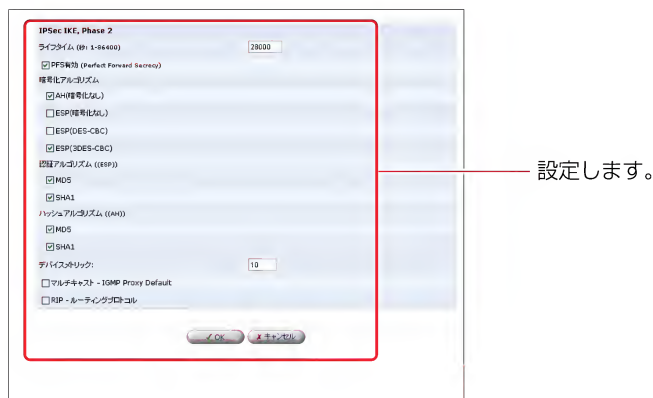
[ハッシュアルゴリズム]

使用するハッシュのアルゴリズムをチェックします。

[Diffie-Hellman-Group]

対応するグループをチェックします。

6 次にIPSec IKE, Phase 2の設定をします。



IPSec IKE, Phase 2

【ライフタイム】

鍵の有効期限を秒単位で設定します。

【PFS有効】

Secrecy(PFS)を使用する場合にチェックします。

【ESP】

暗号ペイロードの設定をします。暗号化アルゴリズムと認証アルゴリズムの設定をします。

【AH】

認証ヘッダの設定をします。ハッシュアルゴリズムを選択します。

【DNSサーバ】

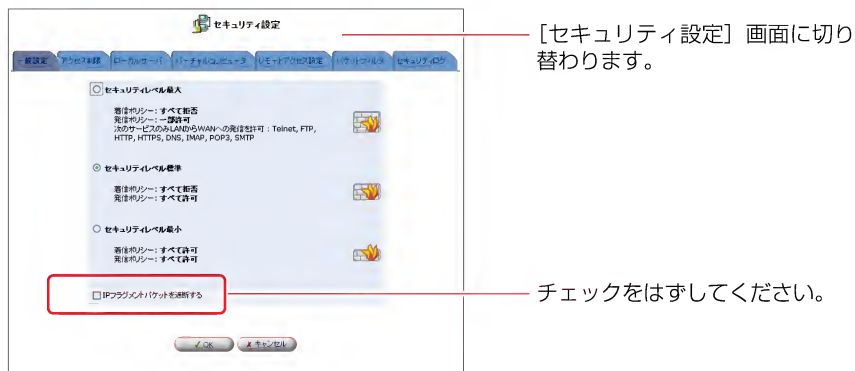
DNSサーバの設定を行います。DNSサーバのIPアドレスを自動的に取得するか、DNSサーバのアドレスを固定設定するかを選択します。固定設定を選択した場合は、プライマリDNSサーバとセカンダリDNSサーバのIPアドレスを入力します。

また、[DNSサーバ]をクリックすると、カスタム設定でDNSサーバを選択した場合と同じ処理を行います。

【デバイスメトリック】

メトリックの値を入力します。

- 7** [詳細設定 VPN IPsec]画面の設定内容を確認し、[OK] ボタンをクリックして、設定を有効にします。
- 8** IPsecを利用しVPNを構築する場合は、IPフラグメントパケットを透過させる必要がありますので、セキュリティ設定画面で、[IPフラグメントパケットを遮断する]のチェックをはずしてください。



■鍵交換方式を手動に設定する場合

鍵交換方式で手動を選択したときは、接続先の設定にあわせて暗号化アルゴリズム、認証アルゴリズムを設定する必要があります。

IPsec 手動鍵交換

セキュリティインデックス - SPI (16進数で入力: 100 - FFFFFFFF)

ローカル: 0

リモート: 0

☐ ローカルとリモートで異なる暗号化キーを使用する

IPsecプロトコル: ESP

暗号化アルゴリズム: 3DES-CBC

キー: [Input field]

認証アルゴリズム: SHA1

サロ: 10

デバイスリンク:

☐ マルチキャスト - IGMP Proxy Default

☐ 利IP - ルーティングプロトコル

OK Cancel

入力します。

暗号化アルゴリズム、認証アルゴリズムのキーは、16進数8桁ずつに区切って入力してください。

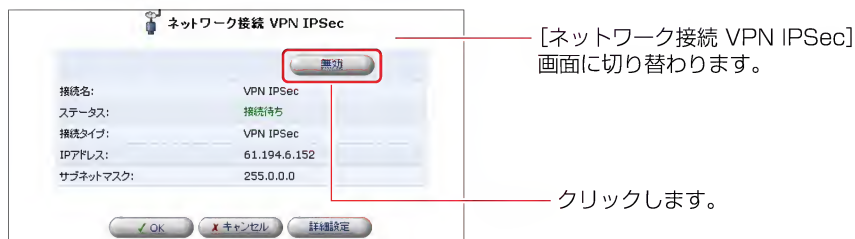
■ VPNの接続、切断

サーバ側、クライアント側でインターネットに接続すると、自動的にLAN同士が接続されます。

- 1 IPsecによる通信を切断したい場合は、[ネットワーク詳細設定] 画面で、[VPN IPsec] の修正ボタンをクリックします。



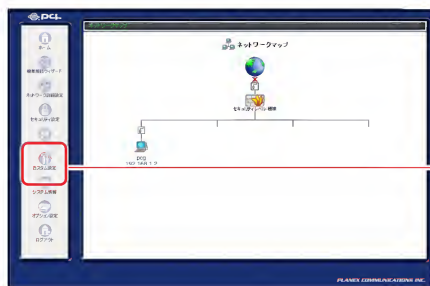
- 2 [ネットワーク接続VPN IPsec] 画面になりますので、[無効] ボタンをクリックします。



IPSec接続に関してその他次の設定が可能です。

■鍵の再生成

- 1 サイドバーから[カスタム設定]アイコンを選択します。



選択します。

- 2 [IPSec]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

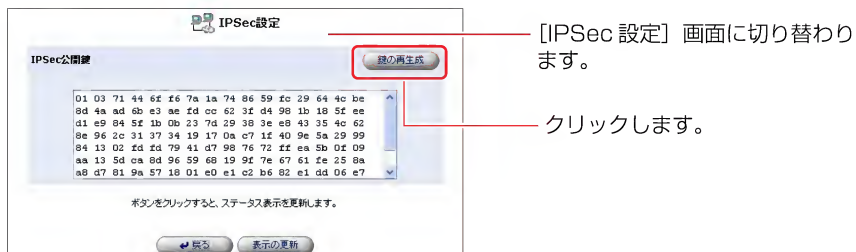
- 3 [IPSec]画面が表示されます。[詳細設定ボタン]をクリックします。



[IPSec] 画面に切り替わります。

クリックします。

- 4 [IPSec 設定]画面が表示されます。[鍵の再生成] ボタンをクリックし、再生成を行います。



- 5 表示の更新ボタンをクリックすると、再生成されたキーが表示されます。[戻る] ボタンをクリックすると [IPSec] 画面に戻ります。

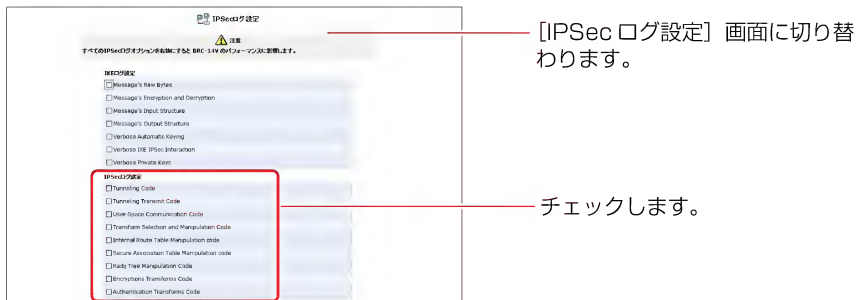
■ IPsec ログの設定

IPsec通信のログに関する設定を変更することができます。

- 1 カスタム設定で [IPsec] アイコンをクリックし、IPsec 画面で [ログ設定] ボタンをクリックします。



- 2 [IPsec ログ設定] 画面が表示されます。記録したい内容にチェックを付けます。

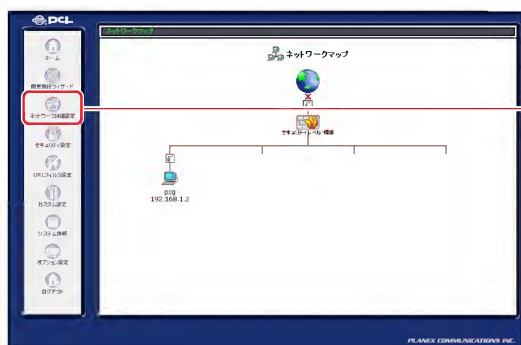


- 3 [OK] ボタンをクリックすると設定が有効になり、[IPsec] 画面に戻ります。

IPSecの削除

ここでは、既に登録してあるIPSec接続を削除する場合について説明します。

1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします



2 [接続名]欄から削除するVPN IPSec接続の[修正]ボタンをクリックします。



[ネットワーク詳細設定] 画面に切り替わります。

修正 ボタンをクリックします。

3 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。



[ネットワーク接続 VPN IPSec] 画面に切り替わります。

クリックします。

クリックします。

- 4** [接続名]欄から削除するVPN IPSec接続の[削除]ボタンをクリックします。



- 5** [戻る]ボタンをクリックします。

- 6** 以上で設定は終了です。

保守・管理


本製品の運用開始後にネットワークの接続状態の確認や、管理者のログイン名やパスワードの変更方法などを説明します。

機器状況の確認

接続状態の確認

各接続ポートごとに通信状態やアドレス情報等が確認できます。

- 1 サイドバーから[システム情報]アイコンをクリックします。



[システム情報] 画面に切り替わります。

接続名	WAN Ethernet	LAN Ethernet	WAN PPPoE
ステータス	接続	接続	接続
物理ポート			WAN Ethernet
通信タイプ	Ethernet	Ethernet	PPPoE
MACアドレス	00:90:cc:00:00:22	00:90:cc:00:00:11	
IPアドレス	192.168.1.1	61.194.6.152	
サブネットマスク	255.255.255.0	255.0.0.0	
デフォルトゲートウェイ		210.153.246.3	
DHCPサーバ		202.239.113.18 202.239.113.26	
DHCPサーバ	無効	有効	
ユーザ名			67840020@f622.sphere.ne.jp
送信/受信	25396	7941	15495
送信/受信	10453	11156	525
送信/受信	35849	18997	16020

[接続状況] 画面には、接続名ごとに、通信の状態やIPアドレス、サブネットマスク、DHCPサーバ機能の使用の有無、DNSサーバのアドレスなどの情報が表示されます。

このボタンをクリックすると、最新の情報に更新されます。

[WAN Ehternet]

PPPoE 以外の方法でインターネットに接続している場合の、WAN 側の通信の状況が確認できます。

[WAN PPPoE]

PPPoE でインターネットに接続している場合の WAN 側の通信の状況が確認できます。

[LAN Ehternet]

LAN 側の通信の状況が確認できます。

[VPN PPTP]

本製品が PPTP クライアントである場合の通信の状況が確認できます。

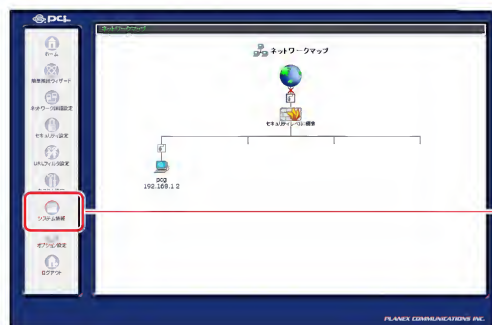
[VPN IPSec]

IPSec で通信している状況が確認できます。

稼働時間の確認

ここでは本製品が稼動してからの現在までの時間を確認できます。

1 サイドバーから[システム情報]アイコンをクリックします。



クリックします。

2 [稼働時間] タブをクリックします。



[稼働時間] 画面に切り替わります。

クリックします。

● 画面表示の自動更新を停止する

[カスタム設定] 画面ー [システム設定] 画面で [システム情報ページの表示の自動更新を行う] をチェックしているときは、[システム情報] の各画面は一定間隔で自動更新されます。このとき、[システム情報] の各画面の [自動更新 Off] ボタンをクリックすると、[今すぐ更新] ボタンをクリックした時のみ、[システム情報] の各画面の内容が更新されるようになります。

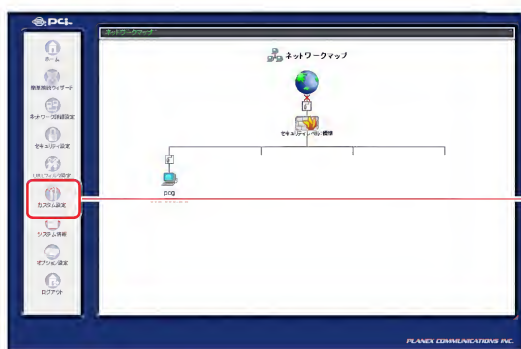
ログインユーザ名・ログインパスワード設定

本製品のログインユーザ名とパスワードの登録、変更、または削除ができます。

ログインユーザ名とログインパスワードの設定

■ユーザの新規作成

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [ユーザ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

[ユーザ] アイコンをクリックします。

3 [ユーザの追加] 欄から「追加」ボタンをクリックします。



4 [ユーザ設定] 画面が表示されます。 フルネーム、ユーザ名、新しいパスワードを入力します。



【フルネーム】

登録するユーザのフルネームを入力します。半角英数字で128桁まで入力できます。

【ユーザ名】

新しく登録するユーザのログイン名を入力します。半角英数字で64桁まで入力できます。

【新しいパスワード】

ユーザがログイン時に使用するパスワードを入力します。半角英数字で64桁まで入力できます。

大文字と小文字は区別されますのでご注意ください。

【新しいパスワードの確認】

「新しいパスワード」と同じパスワードを再度入力します。

5 本製品での権限を設定します。

権限:	<input type="checkbox"/> 管理者権限
	<input type="checkbox"/> PPTP リモートアクセス

[管理者権限]

ユーザを管理者として登録する場合は、チェックします。

[PPTP リモートアクセス]

PPTP による VPN 接続を許可する場合は、チェックします。

6 E-mail 通知を利用する場合は、E-mail アドレス、システム通知レベル、セキュリティ通知レベルを設定します。

E-Mail 通知設定		SMTP メールサーバの設定	
E-Mail アドレス:	<input type="text"/>		
システム通知レベル:	<input type="button" value="なし"/>		
セキュリティ通知レベル:	<input type="button" value="なし"/>		

設定します。

※ E-mail 通知機能に関しては E-mail 通知機能をご参照ください

7 [OK] ボタンをクリックします。

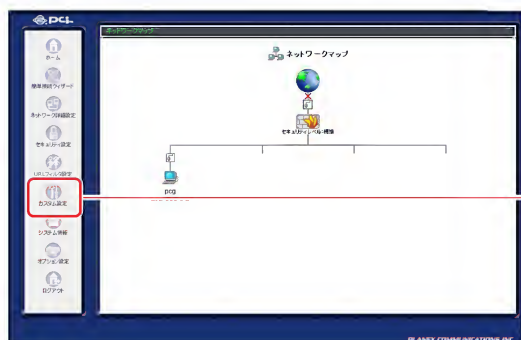
<input type="button" value="OK"/>	<input type="button" value="キャンセル"/>
-----------------------------------	--------------------------------------

クリックします。

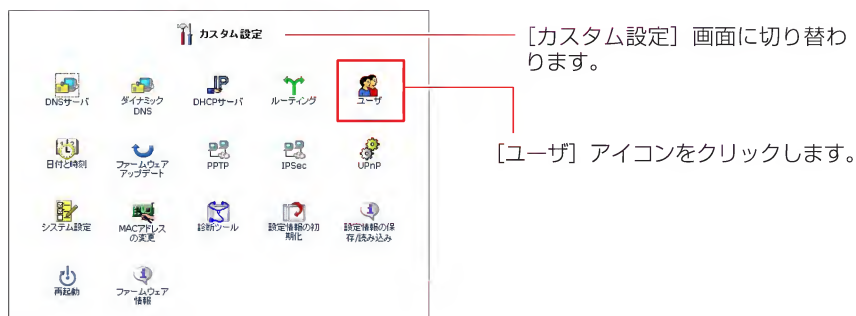
8 以上で設定は終了です。

■ユーザの修正

- 1 サイドバーから[カスタム設定]アイコンをクリックします。




- 2 [ユーザ]アイコンをクリックします。



- 3 設定を変更したいユーザの「修正」ボタンをクリックします。



- 4 [ユーザ設定] 画面が表示されます。修正したい項目の変更を行い、[OK] ボタンをクリックします。

 ユーザ設定 [ユーザ設定] 画面に切り替わります。

一般設定

フルネーム:

ユーザ名 (大文字/小文字に注意):

新しいパスワード:

新しいパスワードの確認:

権限: ☐ 管理者権限
☐ PPTP リモートアクセス

E-Mail通知設定 SMTPメールサーバの設定

E-Mailアドレス:

システム通知レベル: なし ▼

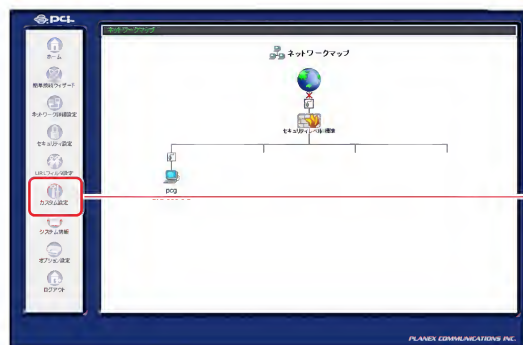
セキュリティ通知レベル: なし ▼

クリックします。

- 5 以上で設定は終了です。

■ユーザの削除

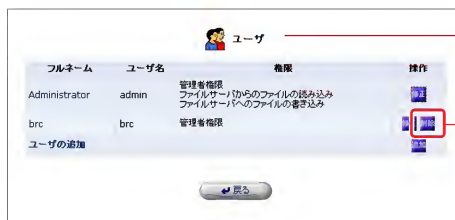
- 1 サイドバーから[カスタム設定]アイコンをクリックします。



- 2 [ユーザ]アイコンをクリックします。



- 3 設定を削除したいユーザの「削除」ボタンをクリックします。



クリックします。

[カスタム設定] 画面に切り替わります。

[ユーザ] アイコンをクリックします。

[ユーザ] 画面に切り替わります。

削除 (削除) ボタンをクリックします。

ご注意

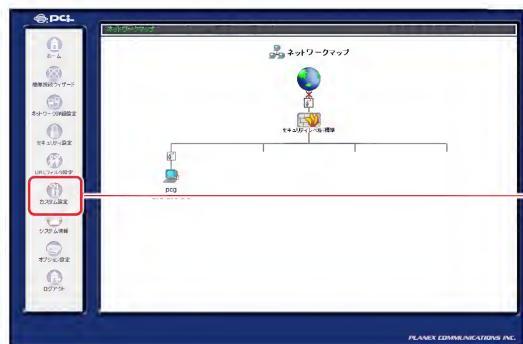
購入時に登録されてる Administrator は削除することができません。

4 以上で設定は終了です。

システム設定

本製品のホスト名やLAN側のドメイン名などを設定できます。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [システム設定]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

[システム設定] アイコンをクリックします。

3 [システム] 欄に本製品のホスト名、ドメイン名を入力します。



[システム設定] 画面に切り替わります。

[システム] 欄に本商品のホスト名、ドメイン名を入力します。

[ホスト名]

本製品のホスト名を入力します。

[ローカルドメイン]

LAN内で使用したいドメイン名を入力します。

4 USBハードディスクを接続している場合、[ファイルサーバ] 欄から [NetBIOSワークグループ名] を入力します。

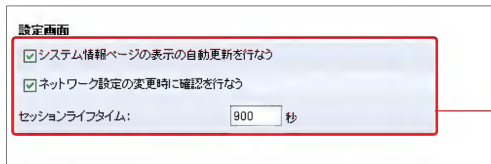


設定します。

[NetBIOSワークグループ名]

LAN内で使用するワークグループ名を入力します。

5 [設定画面] 欄から [システム情報ページの表示の自動更新を行う]、[ネットワーク設定の変更時に確認を行う] を設定します。



設定します。

[システム情報ページの表示の自動更新を行う]

[システム情報] 画面の表示を自動的に更新させたい場合は、チェックします。

[ネットワーク設定の変更時に確認を行う]

ネットワークに関する変更をしたときに、確認メッセージを表示させたい場合は、チェックします。

- 6** [システムリモートログ設定]、[セキュリティリモートログ設定] を利用する場合は設定をします。

システムリモートログ設定

システム通知レベル: なし ▼

セキュリティリモートログ設定

セキュリティ通知レベル: なし ▼

設定します。

※リモートログ設定に関しては、Syslogの設定をご参照ください。

- 7** ユーザ設定でE-mail通知機能を利用している場合は、[SMTPメールサーバ] 欄にメールサーバのアドレスを入力します。

SMTPメールサーバ

SMTPメールサーバ:

送信元メールアドレス:

入力します。

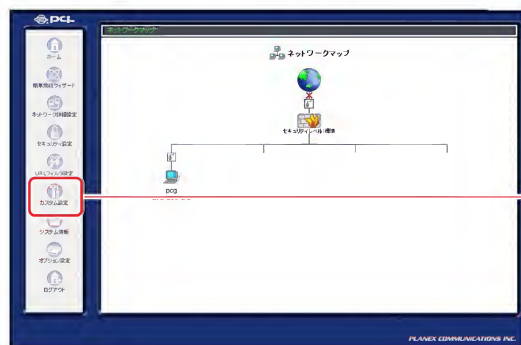
- 8** [OK] ボタンをクリックします。

- 9** 以上で設定は終了です。

日付と時刻の設定

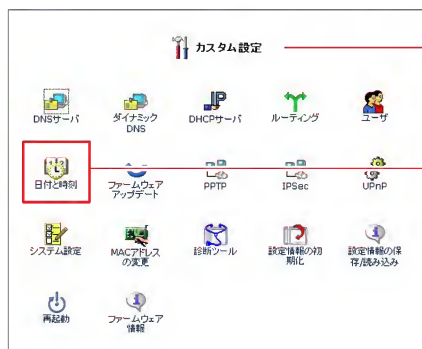
本製品の日付や時刻の設定を変更できます。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [日付と時刻]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

[日付と時刻] アイコンをクリックします。

3 手動設定する場合は、新しい日付と時刻を入力します。

日付と時刻

手動設定

日付: 11月 5 2003

時刻: 14 : 57 : 32

[日付と時刻] 画面に切り替わります。

設定します。

4 自動設定する場合は、[自動設定] 欄から [有効] にチェックします。

自動設定

☒ 有効

プロトコル: ☐ TOD(Time Of Day) ☒ NTP(Network Time Protocol)

更新間隔: 24 時間

NTPサーバアドレス: 210.173.160.87

ステータス: 時刻取得成功

ボタンをクリックすると、ステータス表示を更新します。

OK キャンセル 元の初期値

チェックします。

5 [NTPサーバアドレス]、[ステータス]、[プロトコル]、[更新時間] を入力します。

[NTPサーバアドレス]

指定したアドレスから時刻を指定します。

[プロトコル]

プロトコルの種類。通常はNTPを指定してください。

[更新時間]

時刻を更新する間隔を指定します。

6 [OK] ボタンをクリックします。

7 以上で設定は終了です。

ファームウェアの更新

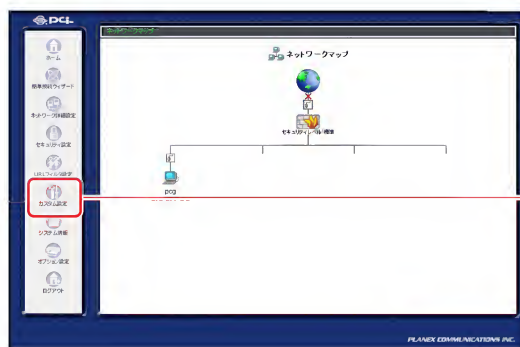
本製品の購入後、当社のホームページからダウンロードしたファイルを使って、最新のファームウェアにアップデートすることができます。

！ ご注意

- ・ インターネットに接続している場合は、アップデートを行う前に全ての通信を切断してください。また、LAN内のパソコンはアップデート作業を行うパソコンを除いて全て電源をOFFにしてください。
- ・ ファイアウォールやウイルススキャンソフトがインストールされてるパソコンでアップデート作業を行う場合は、事前にソフトウェアを終了してください。
- ・ このアップデートは当社が独自に提供するサービスです。新機能の追加や性能の増強を保証するものではありません。

1 当社のホームページから最新のファームウェアをダウンロードします。
ダウンロードしたファイルは、アップデート作業を行うパソコンのハードディスクなどに保存してください。

2 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

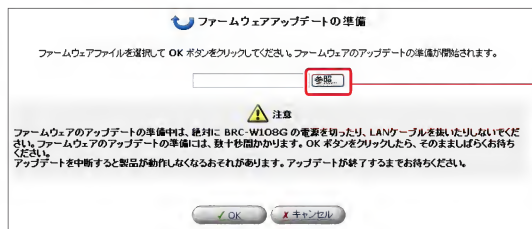
3 [ファームウェアアップデート]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

[ファームウェアアップデート] アイコンをクリックします。

4 [ファームウェアアップデートの準備]の画面が表示されます。 [参照] ボタンをクリックし、ダウンロードしたファームウェアのファイルを指定します。



クリックします。

5 [開く] ボタンをクリックします。



※ Windows® XP のダイアログです。ご使用の OS により、ダイアログは異なります。

クリックします。

- 6** [OK] ボタンをクリックすると、ファームウェアアップデートの準備が開始されます。

! ご注意

ファームウェアアップデートの準備中は、絶対に本製品の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートの準備には、数十秒間かかります。[OK] ボタンをクリックしたら、そのまましばらくお待ちください。

- 7** ファームウェアアップデートの準備が終了すると、[ファームウェアアップデート] の画面が表示されます。
[現在のバージョン] と [新しいバージョン] に表示されるバージョン番号に間違いが無いか確認してください。
[OK] ボタンをクリックすると、ファームウェアのアップデートが開始されます。

! ご注意

ファームウェアのアップデート中は、絶対に本製品の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートには、数十秒間かかります。[OK] ボタンをクリックしたら、そのまましばらくお待ちください。

- 8** アップデートが終了すると、本製品は自動的に再起動します。新しいバージョンのファームウェアは再起動後に有効になります。
- 9** 再起動が完了すると、ログイン画面に戻ります。以上でファームウェアの更新は終了です。

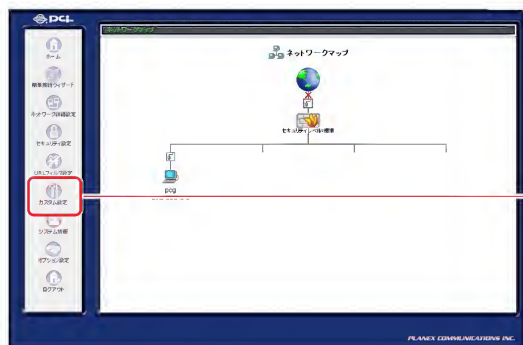
! ご注意

本商品以外のファームウェアを使ってアップデートを行うことはできません。無理にアップデートを行うと本製品が動作しなくなりますので、ご注意ください。

診断ツール

本製品からパソコンなどのネットワーク端末に対してPingを送信することができます。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



クリックします。

- 2 [診断ツール]アイコンをクリックします。



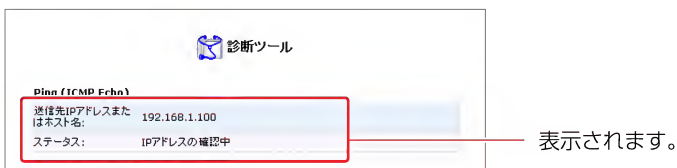
[カスタム設定] 画面に切り替わります。

クリックします。

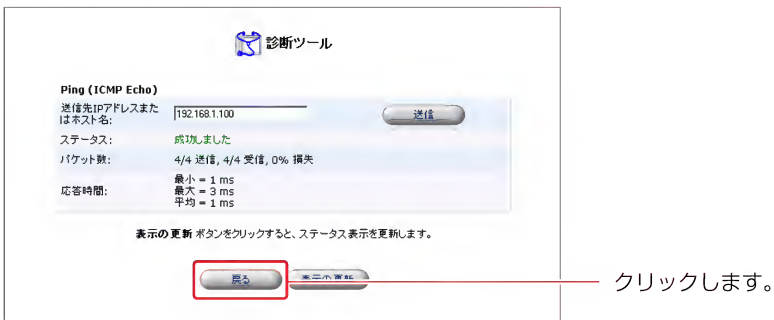
- 3 [送信先IPアドレスまたはホスト名] 欄にPingを送信したいIPアドレスまたはホスト名を入力します。



- 4 [送信] ボタンをクリックすると、本製品から宛先にPingが送信されます。



- 5 [ステータス] 欄に送信結果が表示されます。



- 6 [戻る] ボタンをクリックします。

- 7 以上で設定は終了です。

本製品の初期化

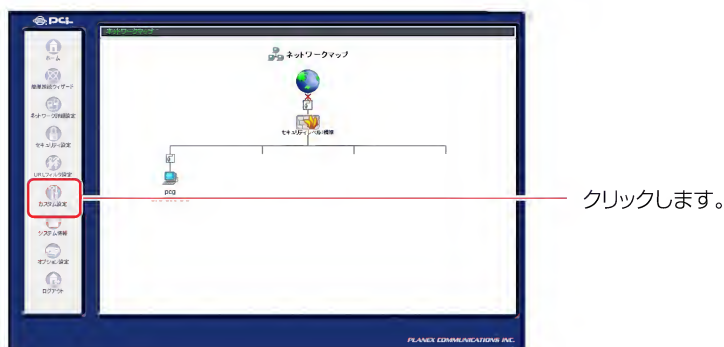
設定ページから本製品の設定内容を消去して、購入時の状態に戻すことができます。

※本体にあるリセットスイッチを使って、設定を消去することもできます。

！ ご注意

この機能を使うと、設定ページにアクセスするためのパスワードを含め、変更した設定内容がすべて消去されます。また、本製品のLAN側ポートのIPアドレスを変更していた場合は、購入時の「192.168.1.1」に戻ります。ご注意ください。

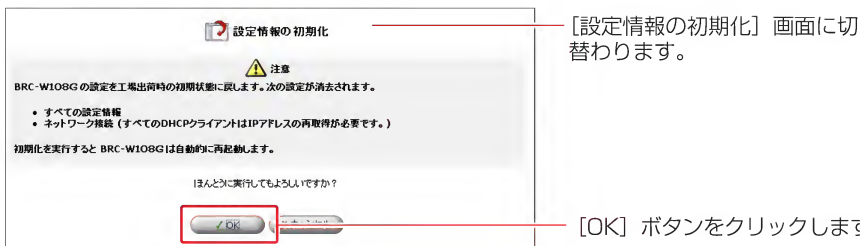
1 サイドバーから[カスタム設定]アイコンをクリックします。



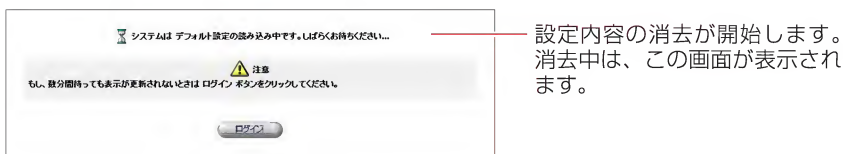
2 [設定情報の初期化]アイコンをクリックします。



3 [OK] ボタンをクリックします。



4 初期化が始まります。



5 設定内容の消去が終わると、設定ページに初めてログインするときの画面に切り替わります。



※ 画面が切り替わらないときは、[ログイン] ボタンをクリックしてください。

- 6** ユーザ名とパスワードを入力し、[OK] ボタンをクリックします。
[ネットワークマップ設定画面] に切り替わります。

[ログインユーザ名]

設定ページにログインするユーザ名を入力します。

[新しいログインパスワード]

パスワードを入力します。

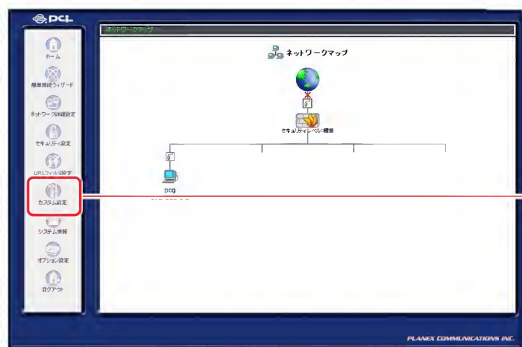
[新しいログインパスワードの確認]

[新しいログインパスワード] の内容をもう一度入力します。

- 7** [OK] ボタンをクリックすると、設定ページの [ネットワークマップ設定画面] に切り替わります。

設定情報の読み込み

- 1 サイドバーから「カスタム設定」アイコンをクリックします。



クリックします。

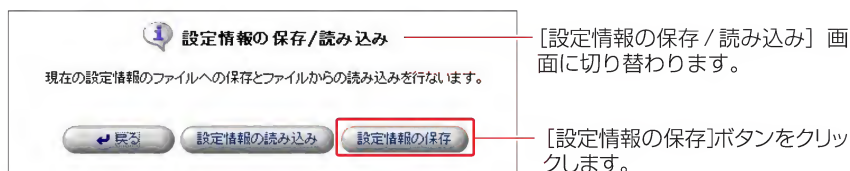
- 2 カスタム設定の「設定情報の保存/読み込み」アイコンをクリックします。



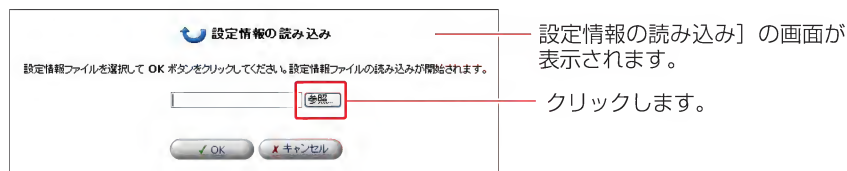
「カスタム設定」画面に切り替わります。

クリックします。

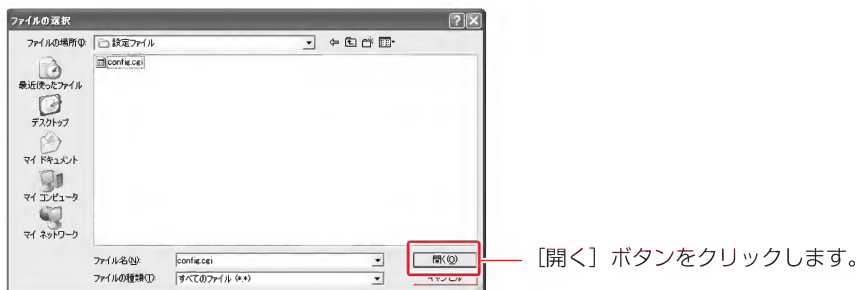
3 「設定情報の読み込み」 ボタンをクリックします。



4 「設定情報の読み込み」の画面が表示されます。 「参照」ボタンをクリックし、設定ファイルを指定します。



5 「開く」ボタンをクリックします。

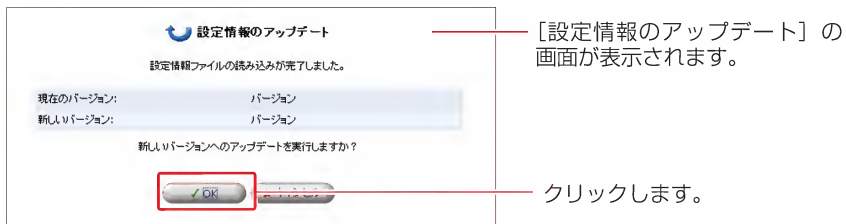


6 「OK」ボタンをクリックすると、設定情報の読み込みの準備が開始されます。

7 設定情報の読み込みの準備が終了すると、[設定情報のアップデート] の画面が表示されます。

[現在のバージョン] と [新しいバージョン] にはファームウェアのバージョンが表示されます。

バージョンが同じことをご確認の上、[OK] ボタンをクリックしてください。



！ **ご注意**

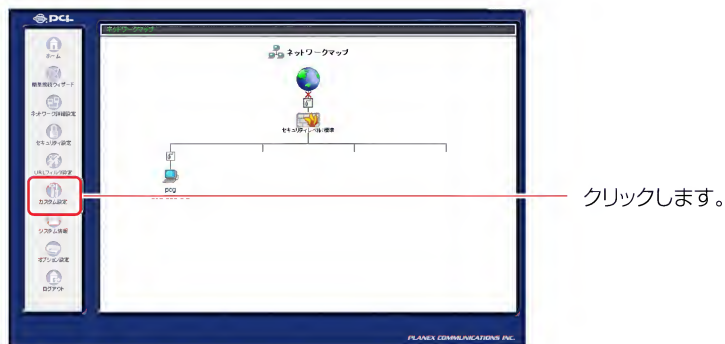
- ・ [現在のバージョン] と [新しいバージョン] にはファームウェアのバージョンが表示されます。
- ・ ファームウェアのバージョンが異なると設定情報のアップデートができない場合がありますのでご注意ください。

8 アップデートが終了すると、本製品は自動的に再起動します。新しい設定情報は再起動後に有効になります。

9 再起動が完了すると、ログイン画面に戻ります。以上で設定情報の読み込みは終了です。

設定情報の保存

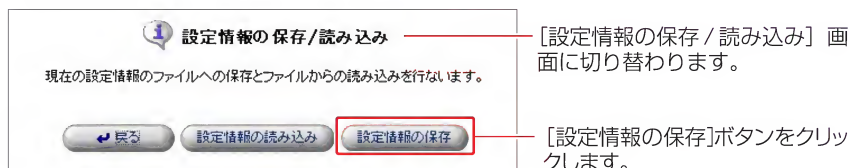
- 1 サイドバーから「カスタム設定」アイコンをクリックします。



- 2 カスタム設定の「設定情報の保存/読み込み」アイコンをクリックします。



- 3 「設定情報の読み込み」ボタンをクリックします。

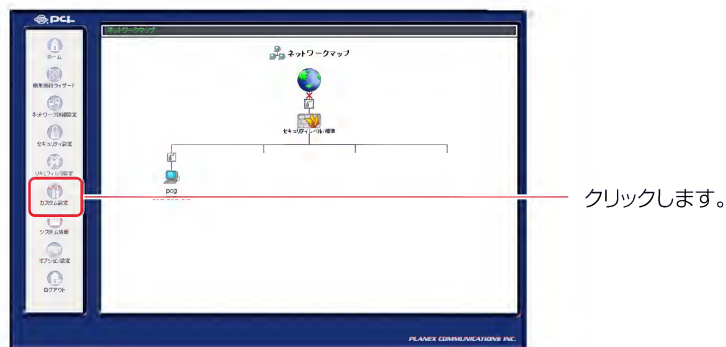


- 4 「ファイルのダウンロード」の画面が表示されます。「保存」ボタンをクリックしてコンピュータに保存します。
- 5 以上で設定情報の保存は終了です。

再起動

本製品の再起動を行います。

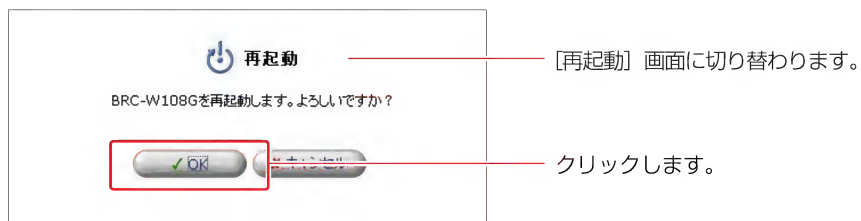
- 1 サイドバーから[カスタム設定]アイコンをクリックします。



- 2 [再起動]アイコンをクリックします。



3 [OK] ボタンをクリックします。

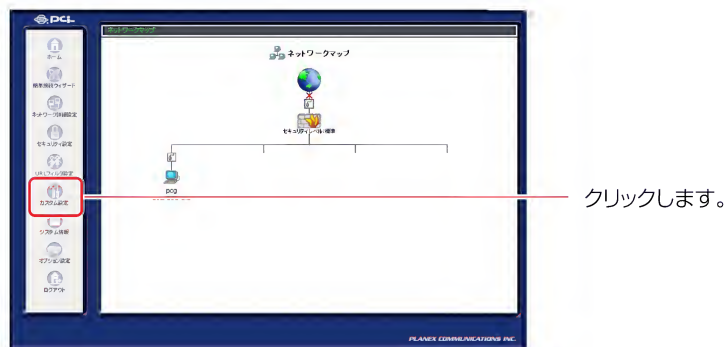


4 再起動が完了すると、ログイン画面に切り替わります。

ファームウェア情報

本製品のファームウェアのバージョンを確認できます。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。



- 2 [ファームウェア情報]アイコンをクリックします。



3 本製品のファームウェアのバージョンが表示されます。



[ファームウェア情報] 画面に切り替わります。